МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный университет»
Колледж

УТВЕРЖДАЮ
директор Колледжа
_____ Д.Ш. Пирбудагова
«14» 03 2022г.

Фонд оценочных средств
по учебной дисциплине

ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Махачкала – 2022

Составитель:

Джафарова З.К. – к.э.н., доцент, преподаватель кафедры общепрофессиональных дисциплин Колледжа ДГУ

Фонд оценочных средств дисциплины рассмотрен и рекомендован к утверждению на заседании кафедры общепрофессиональных дисциплин Колледжа ДГУ.

Протокол №__7__ от «_12_» __03__ 20_22_ г.

Зав.кафедрой общепрофессиональных дисциплин Колледжа ДГУ.
к.ю.н.,доцент _____ Магомедова П. Р

Утверждена на заседании учебно-методического совета колледжа ДГУ

Ст. методист _____ / Шамсутдинова У.А.
подпись *Фамилия И.О.*

ПАСПОРТ фонда оценочных средств
по дисциплине

Основы информационной безопасности

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
1	Раздел I Информационная безопасность в системе национальной безопасности Российской Федерации	ОК 03; ОК 04; ОК 06; ОК 09; ОК 10	Подготовка рефератов; коллоквиум; тестирование; подготовка эссе.
2	Раздел II Информационная война, методы и средства ее ведения	ПК 2.4	Подготовка рефератов; коллоквиум; тестирование; подготовка эссе.
3	Раздел III Обеспечения информационной безопасности компьютерных систем	ОК 03; ОК 06; ОК 09. ПК 2.4	Подготовка рефератов; коллоквиум; тестирование; подготовка эссе.

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	**2**	**3**	**4**
1	Деловая и/или ролевая игра	Совместная деятельность группы обучающихся и педагогического работника под управлением педагогического работника с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема), концепция, роли и ожидаемый результат по каждой игре
2	Кейс-задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.	Задания для решения кейс- задач
3	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования педагогического работника с обучающимися.	Вопросы по темам/разделам дисциплины
4	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Комплект контрольных заданий
5	Круглый стол, дискуссия, полемика, диспут, дебаты	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.	Перечень дискуссионных тем.
6	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио
7	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала.	Образец рабочей тетради
8	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированное™ аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных проектов
9	Разноуровневые задачи и задания	Различают задачи и задания: а) репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; б) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; в) творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разноуровневых задач и заданий

1	2	3	4
10	Расчетно графическая работа/ Лабораторная работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	Комплект заданий для выполнения расчетно-графической работы/ лабораторные работы по темам дисциплин
11	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов
12	Доклад, сообщение	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.	Темы докладов, сообщений
13	Устный опрос/ собеседование/	Средство контроля, организованное как специальная беседа педагогического работника с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
14	Самостоятельная работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	Комплект заданий
15	Презентации	Иллюстрированный материал к выступлению по различной тематике	Темы презентаций
16	Творческое задание	Частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных творческих заданий
17	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
18	Тренажер	Техническое средство, которое может быть использовано для контроля приобретенных студентом профессиональных навыков и умений по управлению конкретным материальным объектом.	Комплект заданий для работы на тренажере
19	Эссе	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием концепций и аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.	Тематика эссе

Критерии оценивания по дисциплине «Основы информационной безопасности»

№ п/п	Наименование оценочного средства	Критерии оценивания на «неудовлетв-но»	Критерии оценивания на «удовлетв-но»	Критерии оценивания на «хорошо»	Критерии оценивания на «отлично»
1	**Деловая и/или ролевая игра**	Не принимает участие в работе группы, не высказывает никаких суждений, не выступает от имени группы; демонстрирует полную неосведомленность по сути изучаемой проблемы	Принимает участие в обсуждении, однако предлагает не аргументированные, не подкрепленные фактическими данными решения; демонстрирует слабую информационную подготовленность к игре	Принимает активное участие в работе группы, участвует в обсуждениях, высказывает типовые рекомендации по рассматриваемой проблеме, готовит возражения оппонентам, однако сам не выступает и не дополняет ответчика; демонстрирует информационную готовность к игре	Принимает активное участие в работе группы, предлагает собственные варианты решения проблемы, выступает от имени группы с рекомендациями по рассматриваемой проблеме либо дополняет ответчика; демонстрирует предварительную информационную готовность в игре
2	**Коллоквиум**	у студента обнаруживается незнание или непонимание большей или наиболее существенной части содержания учебного материала; не способен применять знание теории к решению задач профессионального характера; не умеет определить собственную оценочную позицию; допускает грубое нарушение логики изложения материала. допускает принципиальные ошибки в ответе на вопросы; не может исправить ошибки с помощью наводящих вопросов.	студент в основном знает программный материал в объёме, необходимом для предстоящей работы по профессии, но ответ, отличается недостаточной полнотой и обстоятельностью изложения; допускает существенные ошибки и неточности в изложении теоретического материала; в целом усвоил основную литературу; обнаруживает неумение применять государственно-правовые принципы, закономерности и категории для объяснения конкретных фактов и явлений; требуется помощь со стороны (путем наводящих вопросов, небольших разъяснений и т.п.); испытывает существенные	студент дает ответ, отличающийся меньшей обстоятельностью и глубиной изложения: обнаруживает при этом твёрдое знание материала; допускает несущественные ошибки и неточности в изложении теоретического материала; исправленные после дополнительного вопроса; опирается при построении ответа только на обязательную литературу; подтверждает теоретические постулаты отдельными примерами из юридической практики; способен применять знание теории к решению задач профессионального характера; наблюдается незначительное нарушение логики изложения материала.	студент дает полный и правильный ответ на поставленные и дополнительные (если в таковых была необходимость) вопросы: обнаруживает всестороннее системное и глубокое знание материала; обстоятельно раскрывает соответствующие теоретические положения; демонстрирует знание современной учебной и научной литературы; владеет понятийным аппаратом; демонстрирует способность к анализу и сопоставлению различных подходов к решению заявленной проблематики; подтверждает теоретические постулаты примерами из юридической практики; способен творчески применять знание теории к решению профессиональных задач; имеет собственную оценочную позицию и умеет аргументировано и убедительно ее раскрыть четко излагает материал в логической

			трудности при определении собственной оценочной позиции; наблюдается нарушение логики изложения материала.		последовательности.
3	**Эссе**	тема эссе не раскрыта; материал изложен без собственной оценки и выводов; отсутствуют ссылки на нормативные правовые источники. Имеются недостатки по оформлению работы. Текстуальное совпадение всего эссе с каким-либо источником, то есть – плагиат.	тема раскрывается на основе использования нескольких основных и дополнительных источников; слабо отражена собственная позиция, выводы имеются, но они не обоснованы; материал изложен непоследовательно, без соответствующей аргументации и анализа правовых норм. Имеются недостатки по оформлению.	в целом тема эссе раскрыта; выводы сформулированы, но недостаточно обоснованы; имеется анализ необходимых правовых норм, со ссылками на необходимые нормативные правовые акты; использована необходимая как основная, так и дополнительная литература; недостаточно четко проявляется авторская позиция. Грамотное оформление.	работа отвечает всем предъявляемым требованиям. Тема эссе раскрыта полностью, четко выражена авторская позиция, имеются логичные и обоснованные выводы, написана с использованием большого количества нормативных правовых актов на основе рекомендованной основной и дополнительной литературы. На высоком уровне выполнено оформление работы.
4	**Тест**	0% -50% правильных ответов – оценка «неудовлетворительно»	51% - 64% правильных ответов – оценка «удовлетворительно»	65% - 84% правильных ответов – оценка «хорошо»,	85% - 100% правильных ответов – оценка «отлично»
5	**Лабораторная работа**	студент не осуществил программную реализацию поставленной задачи; студент при программной реализации задачи допустил существенные ошибки, не смог обосновать выбор методов и приемов программирования, ответил не на все поставленные теоретические вопросы.	студент не осуществил программную реализацию поставленной задачи; студент при программной реализации задачи допустил существенные ошибки, не смог обосновать выбор методов и приемов программирования, ответил не на все поставленные теоретические вопросы.	студент в целом осуществил программную реализацию задачи с небольшими недочетами, не обосновал некоторый выбор методов и приемов программирования, ответил не на все поставленные теоретические вопросы. студент осуществил программную реализацию задачи без ошибок, обосновал выбор методов и приемов программирования, ответил на все поставленные теоретические вопросы.	студент в целом осуществил программную реализацию задачи с небольшими недочетами, не обосновал некоторый выбор методов и приемов программирования, ответил не на все поставленные теоретические вопросы; студент осуществил программную реализацию задачи без ошибок, обосновал выбор методов и приемов программирования, ответил на все поставленные теоретические вопросы.

6	**Контрольная работа**	Материал раскрыт не по существу, допущены грубые ошибки в изложении и содержании теоретического материала; контрольная работа выполнена не по установленному варианту.	Вопросы письменной работы в целом раскрыты, но при этом допущена существенная ошибка или ответ неполный, несвязный, однако содержит некоторые обоснованные выводы, которые не в полной мере раскрывают тему.	Вопросы письменной работы раскрыты полностью и правильно, на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки.	Работа соответствует заявленной теме, целям и задачам; характерна: - полнота и конкретность ответа; - последовательность и в изложении материала; - связь теоретических положений с практикой; - высокий уровень анализа и обобщения информационного материала, полноты обзора состояния вопроса; - обоснованность выводов.
7	**Реферат**	Обнаруживается лишь общее представление о теме, либо тема не раскрыта полностью, работа скопирована из Интернета без ссылки на первоисточник.	Вопрос раскрыт частично · Реферат написан небрежно, неаккуратно, использованы не общепринятые сокращения, затрудняющие ее прочтение · Допущено 3-4 фактические ошибки.	Вопрос раскрыт более чем наполовину, но без ошибок. Имеются незначительные и/или единичные ошибки. Использованы ссылки менее чем на половину рекомендованных по данному вопросу источников права Допущены 1–2 фактические ошибки.	Вопрос раскрыт полностью и без ошибок, реферат написан правильным литературным языком без грамматических ошибок в юридической терминологии, умело использованы ссылки на источники права.
8	**Кейс-задача**	Неправильное решение задачи, слабое знание теоретических аспектов, федеральных конституционных законов, федеральных законов и иных актов.	Частично правильное решение задачи, недостаточная аргументация своего решения, определённое знание теоретических аспектов.	Правильное решение задачи, но имеются небольшие недочеты, в целом не влияющие на решение. Решение оформлено без указания на конкретный вид правового акта подлежащего применению в конкретном случае	Правильное решение задачи, подробная аргументация своего решения, знание теоретических аспектов, знание Конституции РФ и федеральных конституционных законов, федеральных законов и иных правовых актов.
9	**Разноуровневые задачи и задания**	Неправильное решение задачи, отсутствие необходимых знание теоретических аспектов решения казуса	Частично правильное решение задачи, недостаточная аргументация своего решение, определённое знание теоретических аспектов решения казуса, частичные ответы на дополнительные вопросы по теме занятия	Правильное решение задачи, достаточная аргументация своего решение, хорошее знание теоретических аспектов решения казуса, частичные ответы на дополнительные вопросы по теме занятия	Правильное решение задачи, подробная аргументация своего решение, хорошее знание теоретических аспектов решения казуса, ответы на дополнительные вопросы по теме занятия

Вопросы для коллоквиумов, собеседования
по дисциплине «Основы информационной безопасности»

Раздел I
Информационная безопасность в системе национальной безопасности Российской Федерации

1. Общие сведения об информационной безопасности
2. Характеристика составляющих "информационной безопасности" применительно к вычислительным сетям.
3. Основные механизмы безопасности.
4. Механизмы безопасности используются для обеспечения конфиденциальности трафика
5. Механизмы безопасности используются для обеспечения "неотказуемости" системы
6. Администрированием средств безопасности
7. Виды избыточности могут использоваться в вычислительных сетях
8. Особенности защиты информации в персональном компьютере.
9. Загрузочный вирус: характерные черты макровируса.
10. Скрытые листы в Excel – признаки заражения макровирусом
11. Наиболее распространенные пути заражения компьютеров вирусами.
12. Особенности заражения компьютеров локальных сетей.
13. Ограничения заражения макровирусом при работе с офисными приложениями
14. Особенности защиты информации в ПК. Угрозы информации в ПК
15. Резидентный вирус
16. Основные этапы алгоритма обнаружения вируса.
17. Особенности заражения вирусами при использовании электронной почты
18. Основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
19. Защита ПК. от несанкционированного доступа.
20. Основные правила защиты от несанкционированного доступа.
21. Составные части IP-адреса
22. Предназначение DNS-сервер
23. Классы удаленных угроз.
24. Программные средства защиты информации.
25. Основные средства защиты информации
26. Основные программные средства защиты информации, дайте основные характеристики.
27. Идентификация и аутентификация.
28. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
29. Идентификация и аутентификация пользователей.
30. Биометрические средства идентификации и аутентификации пользователей.
31. Протоколирование и аудит.
32. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
33. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
34. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.

Раздел II

Информационная война, методы и средства ее ведения

1. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
2. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
3. Административный уровень защиты информации.
4. Процедурный уровень обеспечения безопасности.
5. Авторизация пользователей в информационной системе.
6. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
7. Биометрические средства идентификации и аутентификации пользователей.
8. Криптографические методы защиты
9. Криптология и основные этапы её развития.
10. Основные понятия и определения криптографии.
11. Виды криптосистем.
12. Задачи, решаемые методами криптографии.
13. Виды информации, подлежащие закрытию, их модели и свойства.
14. Частотные характеристики открытых сообщений.
15. Критерии на открытый текст.
16. История криптографии.
17. Основные этапы становления науки криптографии.
18. Методы криптографических преобразований данных.
19. Шифрование заменой.
20. Шифрование перестановкой.
21. Шифрование методом гаммирования и аналитического преобразования.
22. Классификация шифров замены.
23. Шифр Цезаря.
24. Шифр простой замены.
25. Шифр Хилла.
26. Шифр Виженера.
27. Частотный анализ.
28. Стандарты шифрования.
29. Режимы шифрования.
30. Многократное шифрование.
31. Композиция блочных шифров.
32. Совершенные шифры.

Раздел III

Обеспечения информационной безопасности компьютерных систем

1. Пример совершенного шифра.
2. Энтропийные характеристики шифров.
3. Эдеальные шифры.
4. Избыточность языка.
5. Стандарт шифрования DES
6. Стандарт шифрования RSA.
7. Правовое обеспечение защиты информации
8. Международные, российские и отраслевые правовые документы.
9. Концепция правового обеспечения информационной безопасности РФ.
10. Международные правовые акты по защите

информации.
11. Законодательные акты информационной безопасности
12. Федеральный закон «Об информации,
13. информационных технологиях и о защите информации»
14. Шифрование перестановкой.
15. Шифрование методом гаммирования и аналитического преобразования.
16. Многократное шифрование.
17. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров.
20. Идеальные шифры.
21. Стратегия национальной безопасности Российской Федерации: особенности, це ли, составляющие национальных интересов России в информационной сфере.

Контрольно-оценочные материалы для текущего контроля

Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации

Тема 1.1. – Национальная безопасность Российской Федерации

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Национальные интересы РФ и стратегические национальные приоритеты.
4. Цели и смысл государственной службы.
5. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.

Тема 1.2.- Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.

1. Основные составляющие национальных интересов РФ в информационной сфере.
2. Информационная безопасность РФ.
3. Интересы личности в информационной сфере.
4. Интересы общества в информационной сфере.
5. Интересы государства в информационной сфере.
6. Виды угроз информационной безопасности РФ.
7. Источники угроз информационной безопасности РФ.
8. Внешние источники угроз.
9. Внутренние источники угроз.
10. Направления обеспечения информационной безопасности государства.
11. Проблемы региональной информационной безопасности.

Тема 1.3.- Основные понятия и принципы теории информационной безопасности

1. Источники понятий в области информационной безопасности.
2. Основные понятия информационной безопасности: документированная информация, безопасность информации
3. Конфиденциальность, целостность, доступность информации
4. Защита информации, система защиты информации.
5. Принципы теории информационной безопасности.

Тема 1.4. – **Понятие и виды защищаемой информации**

1. Понятие и сущность защищаемой информации.
2. Права и обязанности обладателя информации.
3. Виды защищаемой информации: государственная тайна, служебная тайна,
4. Профессиональная тайна, коммерческая тайна, персональные данные.
5. Перечень сведений конфиденциального характера.
6. Понятие интеллектуальной собственности и особенности ее защиты.

Раздел II. Информационная война, методы и средства ее ведения

Тема 2.1. – Понятие и виды угроз информационной безопасности.

1. Понятие угрозы информационной безопасности.
2. Фактор, воздействующий на защищаемую информацию.
3. Типы дестабилизирующих факторов.
4. Классификация и виды угроз информационной безопасности.
5. Внутренние и внешние источники угроз информационной безопасности.
6. Угрозы утечки информации и угрозы несанкционированного доступа.
7. Основные элементы канала реализации угрозы безопасности информации.

Тема 2.2. – Информационная безопасность и информационное противоборство

1. Субъекты информационного противоборства.
2. Цели информационного противоборства.
3. Составные части и методы информационного противоборства.
4. Информационное оружие, его классификация и возможности.

Тема 2.3. - Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны

1. Методы нарушения конфиденциальности, целостности и доступности информации.
2. Причины, виды, каналы утечки и искажения информации.
3. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
4. Компьютерная система как объект информационной войны.

Раздел III
Обеспечения информационной безопасности компьютерных систем

Тема 3.1.Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны

1. Методы и средства обеспечения информационной безопасности компьютерных систем.
2. Компьютерная система как объект информационной безопасности.
3. Общая характеристика способов и средств защиты информации.
4. Правовая, техническая, криптографическая, физическая защита информации.
5. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.

Тема 3.2. - Механизмы защиты информации в автоматизированных системах

1. Содержание сервисов безопасности программно-технического уровня.
2. Идентификация и аутентификация, управление доступом и авторизация,

протоколирование и аудит.
3. Криптография для сервисов безопасности: шифрование и контроль целостности.
4. Экранирование.
5. Анализ защищенности.
6. Обеспечение доступности.
7. Туннелирование.
8. Управление.

Тема 3.2. – Методы и критерии оценки защищенности компьютерных систем

1. Модели, стратегии и системы обеспечения информационной безопасности.
2. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
3. Критерии безопасности компьютерных систем «Оранжевая книга».
4. Общие критерии безопасности информационных технологий.
5. Защита информации, обрабатываемой в автоматизированных системах от технических разведок.
6. Классификация и возможности технических разведок.
7. Компьютерная разведка.
8. Технические каналы утечки информации при эксплуатации автоматизированных систем.

Самостоятельная работа № 1

Национальная безопасность Российской Федерации

1. Виды безопасности в различных сферах жизнедеятельности личности, общества и государства;
2. Проблемы региональной информационной безопасности;
3. Основные понятия информационной безопасности

Самостоятельная работа № 2 **Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере**.

1. Угрозы информационной безопасности Российской Федерации в различных сферах;
2. Виды защищаемой информации и защита интеллектуальной собственности;
3. Компьютерная система как объект информационной войны

Самостоятельная работа № 3 **Основные понятия и принципы теории информационной безопасности**

1. Механизмы защиты информации компьютерных систем;
2. Проблемы информационной безопасности в государственных структурах;
3. Информационная безопасность в сфере бизнеса

Самостоятельная работа № 4 **Понятие и виды защищаемой информации**

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Влияние процессов информатизации общества на составляющие информационной

безопасности.
3. Состав и содержание направлений информационной безопасности.

Самостоятельная работа № 5 **Понятие и виды угроз информационной безопасности**

1. Государственная информационная политика.
2. История, становление, сущность и содержание, основные направления;
3. Виды информации с точки зрения информационной безопасности.
4. Виды защищаемой информации

Самостоятельная работа № 6 **Информационная безопасность и информационное противоборство**

1. Угрозы информационной безопасности и факторы, воздействующие на информацию;
2. Причины, виды, каналы утечки и искажение информации.
3. Информационное оружие, его классификация и возможности

Самостоятельная работа № 7 **Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны**

1. Методы нарушения конфиденциальности (целостности, доступности) информации
2. Национальные интересы РФ и угрозы национальной безопасности.
3. Угрозы информационной безопасности Российской Федерации.

Самостоятельная работа № 8 **Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны**

1. Политика информационной безопасности предприятия и организации;
2. Организация физической защиты информации.
3. Организация работы с персоналом в системе информационной безопасности

Самостоятельная работа № 9 **Механизмы защиты информации в автоматизированных системах**

1. Актуальные проблемы безопасности компьютерных систем.
2. Актуальные проблемы информационной безопасности при использовании мобильных средств связи;
3. Актуальные проблемы информационной безопасности в социальных сетях.
4. Актуальные проблемы информационной безопасности критически важных объектов.
5. Компьютерная система как объект информационного воздействия

Самостоятельная работа № 10 **Методы и критерии оценки защищенности компьютерных систем**

1. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
2. Современные методы и средства защиты информации.
3. Отечественные и зарубежные стандарты в области информационной безопасности.;

4. Криптология и основные этапы ее становления и развития.
5. Комплексный подход к обеспечению информационной безопасности.
6. Основные механизмы и сервисы защиты информации.
7. Правовое обеспечение информационной безопасности

Перечень дискуссионных тем для круглого стола
(дискуссии, полемики, диспута, дебатов)
по дисциплине

Темы эссе
(рефератов, докладов, сообщений)

1. Понятие безопасности и защиты информации.
2. Понятие политики безопасности информационных систем. Назначение политики
3. безопасности.
4. Основные типы политики безопасности доступа к данным.
5. Законодательный уровень обеспечения информационной безопасности.
6. Основные законодательные акты РФ в области защиты информации.
7. Функции и назначение стандартов информационной безопасности.
8. Основные положения «Доктрины информационной безопасности РФ».
9. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
10. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
11. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
12. Биометрические средства идентификации и аутентификации пользователей.
13. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
14. Законодательный уровень применения цифровой подписи.
15. Информационная сфера и ее элементы.
16. Понятие безопасности и информационной безопасности.
17. Основные составляющие информационной безопасности.
18. Субъекты и объекты правоотношений в области информационной безопасности.
19. Концептуальные положения организационного обеспечения информационной безопасности.
20. Понятие и виды угроз безопасности.
21. Угрозы информационной безопасности на объекте.
22. Организация службы безопасности объекта
23. Правовой режим информации: понятие, признаки, содержание.
24. Виды информации ограниченного доступа.
25. Требования, предъявляемые к организации защиты конфиденциальной информации.
26. Виды компьютерных преступлений.
27. Особенности квалификации компьютерных преступлений.
28. Преступления имущественного характера, которые совершаются с применением или в отношении средств компьютерной техники.
29. Характеристика видов правового режима информации с точки зрения его обязательности и объекта.
30. Общий правовой режим информации.
31. Специальные правовые режимы информации.
32. Тайна как специальный правовой режим.

33. Конфиденциальность как специальный правовой режим.
34. Государственная тайна и ее защита.
35. Защита персональных данных.
36. Защита коммерческой тайны.
37. Профессиональная тайна.
38. Служебная тайна.
39. Виды информационного законодательства, применяемые для регулирования отношений в Интернет.
40. Угроза безопасности, обеспечение безопасности: понятие.
41. Информационная безопасность: понятие, первоочередные меры по обеспечению, общие методы.
42. Информационная безопасность и информационные войны: понятие.
43. Информационная безопасность и информационное оружие: понятие.
44. Правонарушение и информационное правонарушение: определение, признаки, юридическая ответственность и основание привлечения к ответственности.
45. Состав информационного правонарушения.
46. Уголовная ответственность за информационное преступление.
47. Административная и гражданско-правовая ответственность в информационной сфере.

Комплект тестов (тестовых заданий) по дисциплине
«Организационно-правовое обеспечение информационной безопасности»

1. По типу возникновения угрозы безопасности информации принято делить на
- случайные и умышленные
- активные и пассивные
- регламентированные и нерегламентированные
- уголовные и административные
2. Основная угроза безопасности информации – раскрытие конфиденциальной – информации
выражается в
- несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
- получении одним из абонентов сведений, доступ к которым ему запрещен
- непризнании получателем или отправителем информации фактов ее получения или отправки
3. Основная угроза безопасности информации – компрометация информации выражается в
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден
либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
- несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб
- получении одним из абонентов сведений, доступ к которым ему запрещен
- непризнании получателем или отправителем информации фактов ее получения или отправки

4. Основная угроза безопасности информации – несанкционированный обмен информацией между абонентами выражается в
- получении одним из абонентов сведений, доступ к которым ему запрещен
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден
либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и
восстановления истинных сведений
- несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб
5. Основная угроза безопасности – информации отказ от информации выражается в
- непризнании получателем или отправителем информации фактов ее получения или отправки
- получении одним из абонентов сведений, доступ к которым ему запрещен
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
- несанкционированном доступе к БД, прослушивании каналов и т.п., т.е. это получение информации, являющейся достоянием некоторого лица другими лицами, в результате чего владельцам информации наносится существенный ущерб
6. Основная угроза безопасности информации – отказ в обслуживании выражается в
- неправильной работе самой ИС, является весьма существенной и распространенной угрозой
- непризнании получателем или отправителем информации фактов ее получения или отправки
- получении одним из абонентов сведений, доступ к которым ему запрещен
- внесении несанкционированных изменений в БД, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринять дополнительные усилия для выявления изменений и восстановления истинных сведений
7. Препятствие – это метод защиты информации путем
- физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.)
- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
8. Управление доступом – это метод защиты информации путем
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и

использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
9. Маскировка – это метод защиты информации путем
- ее криптографического закрытия
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
- физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.)
10. Регламентация – это метод защиты информации путем
- создания такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму
- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
11. Принуждение – это метод защиты информации путем
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий;
- разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
12. Побуждение – это метод защиты информации путем
- побуждения пользователей ИС не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных
- регулирования использования всех ресурсов ИС и выполнения таких функций как идентификация объекта, опознание объекта по предъявленному им идентификатору, проверку полномочий; разрешение и создание условий работы в пределах установленного регламента, регистрацию обращений к защищаемым ресурсам, регулирование при попытках несанкционированных действий
- вынуждения пользователей и персонала ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
- физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.)
13. В главе 28 "Преступления в сфере компьютерной информации" УК РФ определяются следующие общественно-опасные деяния в отношении средств компьютерной техники:
- неправомерный доступ к охраняемой законом компьютерной информации; создание

вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
- финансовое мошенничество; кража конфиденциальной информации; мошенничество, касающееся средств связи; несанкционированный доступ; диверсия; проникновение в систему
- несанкционированный доступ к информации; применение не сертифицированных программ и баз данных; создание вирусных программ
14. Основными мотивами при совершении компьютерных преступлений являются
- корыстные, политические, исследовательский интерес, хулиганство и озорство, месть
- корыстные, политические
- хулиганство и озорство
-месть
15. Основными опасными субъектами неправомерного доступа к компьютерной информации
являются
- все верны
- хакеры-исследователи, хакеры взломщики, хакеры-вандалы
- крэкеры, компьютерные пираты, кибертеррористы
- вирмейкеры, кардеры, фрикеры
16. Хакеры-исследователи – люди
- образованные и талантливые, основным занятием которых является анализ разнообразного программного обеспечения на уязвимости, которыми может воспользоваться потенциальный взломщик или которые могут улучшить работу компьютерной системы, сети, увеличивая ее эффективность
- осуществляющие по различным целям взлом, проникновение, при котором никакая информация не была уничтожена на каких-либо носителях, система продолжала работать без снижения своей эффективности, после проникновения хакер сообщил соответствующим лицам, ответственным за безопасность данной системы о проникновении, способе проникновения и подробно описал процедуру вторжения
-специализирующиеся на изучении особенностей кредитных карт и банкоматов
17. Хакеры-взломщики – люди
- осуществляющие по различным целям взлом, проникновение, при котором никакая информация не была уничтожена на каких-либо носителях, система продолжала работать без снижения своей эффективности, после проникновения хакер сообщил соответствующим лицам, ответственным за безопасность данной системы о проникновении, способе проникновения и подробно описал процедуру вторжения
- по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
18. Хакеры-вандалы – люди
- по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
- которые специализируются на взломе программного обеспечения для последующей продажи
19. Крэкеры – люди
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
- чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи

- которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб

20. Компьютерные пираты – люди

- чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
- по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам

21. Кибертеррористы – люди

- которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб
- по каким-то причинам планирующие и осуществляющие вторжение в компьютерные системы с сознательной целью причинения ущерба этим системам
- чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях

22. Вирмейкеры – люди

- которые занимаются написанием компьютерных вирусов
- которые целенаправленно стараются причинить вред государству или какой-то группе людей, по идеологическим соображениям, по возможности, максимизируя причиненный ущерб
- чаще всего группы, которые специализируются на взломе программного обеспечения для последующей продажи

23. Кардеры – люди - специализирующиеся на изучении особенностей кредитных карт и банкоматов

- специализирующиеся на изучении особенностей незаконного подключения к линиям связи
- которые занимаются написанием компьютерных вирусов

24. Фрикеры – люди

- специализирующиеся на изучении особенностей незаконного подключения к линиям связи
- специализирующиеся на изучении особенностей кредитных карт и банкоматов
- которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях

25. По типу возникновения угрозы безопасности информации принято делить на

- случайные и умышленные
- активные и пассивные
- регламентированные и нерегламентированные
- уголовные и административные

26. Правонарушителей в области компьютерной преступности по социальному статусу и уровню
образования можно разделить на следующие группы

- ученики школ; студенты; сотрудники высших учебных заведений;
- кассиры банков; программисты
- лица, состоящие с потерпевшим в трудовых или иных деловых отношениях; лица, не связанные деловыми отношениями с потерпевшим

-хакеры-исследователи, хакеры взломщики, хакеры-вандалы все верны

27. С точки зрения уголовно-правовой охраны под компьютерными преступлениями следует понимать
- предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства
- нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (т.е. машинной информации)
- предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники
28. С точки зрения криминалистических аспектов под компьютерными преступлениями следует понимать
- предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники
- предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства
- нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (т.е. машинной информации)
29. К методам обеспечения информационной безопасности не относятся:
а) корпоративные;
б) административные;
в) правовые;
г) технические.
30. Какие методы не относятся к обеспечению информационной безопасности:
а) принуждение и побуждение;
б) управление доступом и регламентация;
в) маскировка и препятствие;
г) скрытый доступ и копирование сообщений.
31. Методы защиты информации можно разбить:
а) на три большие группы;
б) на две большие группы;
в) на четыре большие группы;
г) на пять больших групп.
32. Методы, не имеющие математического обоснования стойкости, часто называют методами:
а) С чѐрным ящиком;
б)С белым квадратом;
в) С желтым кругом;
г) Нет верного ответа.
33. Методы, функционирующие по принципу "черного ящика", называют
а) SecurityThroughObscurity;
б) System ThroughObscurity;
в) SecurityThrough;
г) SystemObscurity.
34. Метод физического преграждения пути злоумышленнику к информации:
а) управление доступом;
б) маскировка;
в) принуждение;
г) побуждение.
35. Метод защиты информации путем ее криптографического преобразования:
а) Принуждение;
б) Побуждение;

в) Маскировка;
г) управление доступом.
36. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:
а) Уполномочивание;
б)Контроль доступа;
в) Сертификация;
г) Нет верного ответа.
37. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:
а) уязвимость;
б) атака;
в) угроза;
г) нет верного ответа.
38. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого еѐ состояния, при котором создаются условия для реализации угроз безопасности информации - это:
а) атака;
б) угроза;
в) уязвимость;
г) статичность.
39. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:
а) статичность;
б) атака;
в) угроза;
г) изъян.
40. Какая угроза отказа служб устраняется административно-правовыми методами;
а) отказ пользователей;
б) отказ программного обеспечения;
в) нарушение работ систем связи;
г) разрушение и повреждение помещений
41. К каналам, предполагающим изменение элементов информационной структуры относится:
а) намеренное копирование файлов и носителей информации;
б) маскировка под других пользователей, путѐм похищения идентифицирующей их информации;
в) хищение носителей информации;
г) незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.
42. Что относится к каналам, не требующим изменение элементов ИС?
а) намеренное копирование файлов и носителей информации;
б) незаконное подключение специальной регистрирующей аппаратуры;
в) злоумышленное изменение программ;
г) злоумышленный вывод из строя средств защиты информации.
43. Какая направленность атак неверно сформулирована?
а) атаки на уровне операционной системы;
б) атаки на уровне системного администратора;
в) атаки на уровне сетевого программного обеспечения;
г) атаки на уровне систем управления базами данных.
44. К какому типу атак относится прослушивание передаваемых сообщений:
а) Пассивная атака;

б) Модификация потока данных;
в) Повторное использование;
г) Отказ в обслуживании.
45. Политика безопасности это:
а) это одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности;
б) формальная спецификация правил и рекомендаций, на основе которых пользователи используют, накапливают и распоряжаются информационными ресурсами и технологическими ценностями;
в) - набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации;
г) верны все варианты.
46. Метод защиты информации путем ее криптографического преобразования:
а) Принуждение;
б) Побуждение;
в) Маскировка;
г) управление доступом.
47. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:
а) Уполномочивание;
б)Контроль доступа;
в) Сертификация;
г) Нет верного ответа.
48. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:
а) уязвимость;
б) атака
в) угроза;
г) нет верного ответа
49. Какой официальный документ занимает главное место в системе законодательства в области авторского права РФ?
а) Конституция РФ;
б) Уголовный Кодекс РФ;
в) Гражданский Кодекс;
г) Трудовой Кодекс.
50. Как называется Федеральный Закон, регулирующий авторские и смежные права в РФ?
а) Закон РФ "О персональных данных";
б) Закон РФ "Об авторском праве и смежных правах";
в) Закон РФ "О защите прав потребителей".
51. Под способами защиты авторских и смежных прав понимаются?
а) закрепленные законом материально-правовые меры принудительного характера, посредством которых производится восстановление (признание) нарушенных (оспариваемых) прав и воздействие на правонарушителя;
б) закрепленные законом материально-правовые меры принудительного характера, посредством которых производится восстановление (признание) нарушенных (оспариваемых) прав и отсутствует воздействие на правонарушителя;
в) закрепленные законом материально-правовые меры принудительного характера, посредством которых происходит воздействие на правонарушителя и не производится восстановление (признание) нарушенных (оспариваемых) прав.

52. В соответствии со ст. 49 Закона РФ "Об авторском праве и смежных правах" обладатели исключительных авторских и смежных прав вправе потребовать от нарушителя:
а) признания прав;
б) восстановления положения, существовавшего до нарушения права;
в) прекращения действий, нарушающих право или создающих угрозу его нарушению;
г) все верны варианты.
53. В соответствии со ст. 49 Закона РФ "Об авторском праве и смежных правах" обладатели исключительных авторских и смежных прав вправе потребовать от нарушителя:
а) возмещения убытков;
б) взыскания дохода, полученного нарушителем вследствие нарушения авторских и смежных прав;
в) выплаты компенсации в определенных законом пределах;
г) все верны варианты.
54. Согласно п. 2 ст. 49 Закона РФ "Об авторском праве и смежных правах" помимо возмещения убытков, взыскания незаконного дохода или выплаты компенсации в твердой сумме суд или арбитражный суд за нарушение авторских или смежных прав взыскивает штраф в размере___% суммы, присужденной судом в пользу истца:
а) 5%;
б) 10%;
в) 15%;
г) 20%.
55. Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с:
а) Гражданским кодексом Российской Федерации;
б) Федеральным законом "Об информации, информатизации и защите информации";
в) Федеральным законом "О связи";
г) верны все варианты.
56. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:
а) сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
б) подтверждена подлинность электронной цифровой подписи в электронном документе;
в) электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи;
г) верны все варианты.

57. Создание ключей электронных цифровых подписей осуществляется для использования в:
а) информационной системе общего пользования ее участником или по его обращению удостоверяющим центром;
б) корпоративной информационной системе в порядке, установленном в этой системе;
в) верны оба варианты.
58. При передаче документов, содержащих коммерческую тайну, в органы государственной власти и органы местного самоуправления гриф «Коммерческая тайна» или «Конфиденциально» проставляется:
а) в обязательном порядке;
б) в желательном порядке;
в) в не обязательном порядке.

59.Объектом правового режима коммерческой тайны является:
а) только научно-техническая и технологическая (в том числе составляющая секреты производства — ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;
б) только производственная и финансово-экономическая информация (в том числе составляющая секреты производства — ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;
в) научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства — ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении, которой обладателем такой информации введен режим коммерческой тайны.
60. В целях охраны конфиденциальности информации работодатель обязан:
а) ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;
б) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;
в) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны;
г) верны все варианты.
61.В целях охраны конфиденциальности информации работник обязан:
а) выполнять установленный работодателем режим коммерческой тайны;
б) не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;
в) не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем, заключенным в период срока действия трудового договора, или в течение трех лет после прекращения трудового договора, если указанное соглашение не заключалось;
г) верны все варианты.
62. На документах, предоставляемых указанным органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф:
а) «Коммерческая тайна»;
б) «Служебная тайна»;
в) «Деловая тайна».
63. В соответствии со ст. 49 Закона РФ "Об авторском праве и смежных правах" обладатели исключительных авторских и смежных прав вправе требовать от нарушителя:
а) признания прав;
б) восстановления положения, существовавшего до нарушения права;
в) прекращения действий, нарушающих право или создающих угрозу его нарушению;
г) верны все варианты.

64. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:
а) сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
б) подтверждена подлинность электронной цифровой подписи в электронном документе;
в) электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.
г) верны все варианты.
65. Какая из перечисленных задач не является государственной системой защитой информации?
а) проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;
б) исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных специальных программно-технических воздействий на информацию с целью ее разрушения, уничтожения, искажения или блокирования в процессе обработки, передачи и хранения;
в) принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области защиты информации;
г) принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области вредоносных носителей.
66. Что из перечисленного не входит в первый уровень правового обеспечения информационной безопасности:
а) Конституция РФ (ст. 23, право на тайну переписки);
б) Гражданский кодекс РФ (ст. 139, возмещение убытков от утечек);
в) Федеральный закон "О государственной тайне";
г) Постановления Правительства РФ.
67. При передаче документов, содержащих коммерческую тайну, в органы государственной власти и органы местного самоуправления гриф «Коммерческая тайна» или «Конфиденциально» проставляется:
а) в обязательном порядке;
б) в желательном порядке;
в) в не обязательном порядке.
68. Из скольких уровней состоит правовое обеспечение информационной безопасности:
а) двухуровней;
б) трех уровней;
в) четырех уровней;
г) пяти уровней.
69. Как называется стандарт ГОСТ Р ИСО/МЭК 15408-1—2002?
а) Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
б) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
в) Защита информации. Основные термины и определения;
г) Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель.
70. Как называется стандарт ГОСТ Р 50739-95?
а) Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;

б) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
в) Защита информации. Основные термины и определения;
г) Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель.
71. Как называется стандарт ГОСТ Р 50922-96?
а) Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
б) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
в) Защита информации. Основные термины и определения;
г) Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
72. Как называется стандарт ГОСТ Р ИСО 7498-2-99?
а) Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
б) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
в) Защита информации. Основные термины и определения;
г) Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель.
73. В состав стандарта ГОСТ Р ИСО/МЭК 15408-2002 входят следующие части?
а) Часть 1 (ГОСТ Р ИСО/МЭК 15408-1 «Введение и общая модель»;
б) Часть 2 (ГОСТ Р ИСО/МЭК 15408-2 «Функциональные требования безопасности»);
в) Часть 3 (ГОСТ Р ИСО/МЭК 15408-3 «Требования доверия к безопасности»);
г) верны все варианты.
74. Назовите главные достоинства стандарта ГОСТ Р ИСО/МЭК 15408:
а) полнота требований к ИБ;
б) гибкость в применении;
в) открытость для последующего развития с учетом новейших достижений науки и техники;
г) верны все варианты.
75. Какой из ниже представленных стандартов обеспечения защиты информации не является отечественным?
а) ISO/IEC 17799:2002 (BS 7799:2000)
б) ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель.
в) ГОСТ Р 50739-95Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
г) ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
76. Информацию по степени доступа разделяют на:
а) открытую и ограниченного доступа;
б) открытую;
в) закрытую;
г) тайную и ограниченную.
77. К информации ограниченного доступа относятся:
а) государственная тайна;
б) конфиденциальная информация;
в) персональные данные;
г) все ответы верны.

78. Информационная безопасность являются переводом на русский язык английского термина:
а) informationsecurity;
б)informationsystem;
в) informationcurrency;
г) informationcrypto.
79. Защитой информации называют:
а) деятельность по предотвращению утечки любой информации;
б) деятельность по предотвращению утечки защищаемой информации;
в) деятельность по предотвращению утечки доступной информации;
г) все ответы верны.
80. Под утечкой понимают:
а) неконтролируемое распространение защищаемой информации путем ее разглашения или несанкционированного доступа к ней; б) неконтролируемое распространение скрытой информации путем еѐ разглашения или несанкционированного доступа к ней;
в) неконтролируемое распространение конфиденциальной информации путем ее разглашения или несанкционированного доступа к ней;
г) все верно.
81. Под непреднамеренным воздействием на защищаемую информацию понимают:
а) воздействие на неѐ из-за ошибок пользователя, сбоя технических или программных средств, иных нецеленаправленных действий;
б) воздействие на неѐ из-за ошибок пользователя, сбоя технических средств;
в) воздействие на неѐ из-за ошибок пользователя, программных средств, иных нецеленаправленных действий;
г) все ответы верны.
82. Что не является характеристикой информации:
а) статичность;
б) тип доступа;
в) время отклика;
г) стоимость создания.
83. К наиболее распространѐнным правонарушениям в сети Internet не относится:
а) мошенническая деятельность;
б) перлюстрация частной переписки;
в) нарушение авторских и смежных прав;
г) нелегальное получение товаров и услуг.
84. Что не относится к задачам информационной безопасности:
а) целостность и секретность;
б) электронная подпись и датирование;
в) устойчивость связи и определение трафика;
г) анонимность.
85. К методам обеспечения информационной безопасности не относятся:
а) корпоративные;
б) административные;
в) правовые;
г) технические.
86. Какие методы не относятся к обеспечению информационной безопасности:
а) принуждение и побуждение;
б) управление доступом и регламентация;
в) маскировка и препятствие;
г) скрытый доступ и копирование сообщений.

87. Методы защиты информации можно разбить:
а) на три большие группы;
б) на две большие группы;
в) на четыре большие группы;
г) на пять больших групп.
88. Метод физического преграждения пути злоумышленнику к информации:
а) управление доступом;
б) маскировка;
в) принуждение;
г) побуждение.
89. К методам обеспечения информационной безопасности не относятся:
а) корпоративные;
б) административные;
в) правовые;
г) технические.
90. Какие методы не относятся к обеспечению информационной безопасности:
а) принуждение и побуждение;
б) управление доступом и регламентация;
в) маскировка и препятствие;
г) скрытый доступ и копирование сообщений.
91. Методы защиты информации можно разбить:
а) на три большие группы;
б) на две большие группы;
в) на четыре большие группы;
г) на пять больших групп.
92. Методы, не имеющие математического обоснования стойкости, часто называют методами:
а) С чѐрным ящиком;
б)С белым квадратом;
в) С желтым кругом;
г) Нет верного ответа.
93. Методы, функционирующие по принципу "черного ящика", называют
а) SecurityThroughObscurity;
б) System ThroughObscurity;
в) SecurityThrough;
г) SystemObscurity.
94. Метод физического преграждения пути злоумышленнику к информации:
а) управление доступом;
б) маскировка;
в) принуждение;
г) побуждение.
95. Метод защиты информации путем ее криптографического преобразования:
а) Принуждение;
б) Побуждение;
в) Маскировка;
г) управление доступом.
96. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:
а) Уполномочивание;
б) Контроль доступа;
в) Сертификация;
г) Нет верного ответа.

97. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:
а) уязвимость;
б) атака;
в) угроза;
г) нет верного ответа.
98. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации - это:
а) атака;
б) угроза;
в) уязвимость;
г) статичность.
99. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:
а) статичность;
б) атака;
в) угроза;
г) изъян.
100. Какая угроза отказа служб устраняется административно-правовыми методами:
а) отказ пользователей;
б) отказ программного обеспечения;
в) нарушение работ систем связи;
г) разрушение и повреждение помещений
101Фрикеры – люди
a. + специализирующиеся на изучении особенностей незаконного подключения к линиям связи
b. + субъекты, специализирующиеся на совершении преступлений в области электросвязи с использованием конфиденциальной компьютерной информации и специальных технических средств, разработанных (приспособленных, запрограммированных) для негласного получения (модификации, блокирования) информации с технических каналов электросвязи.
c. - специализирующиеся на изучении особенностей кредитных карт и банкоматов
d. - которые целенаправленно занимаются коммерческим взломом компьютерных систем и сетей в корыстных целях
e. - которые оплачивают свои покупки чужой банковской картой, платёжными реквизитами которой они смогли завладеть
f. - специализирующиеся на изучении особенностей кредитных карт и банкоматов
102.Кардеры – люди
a. + которые оплачивают свои покупки чужой банковской картой, платёжными реквизитами которой они смогли завладеть.
b. + специализирующиеся на изучении особенностей кредитных карт и банкоматов
c. - специализирующиеся на изучении особенностей незаконного подключения к линиям связи
d. - которые занимаются написанием компьютерных вирусов
e. - специализирующиеся на изучении особенностей незаконного подключения к линиям связи
f. - специализирующиеся на совершении преступлений в области электросвязи с использованием конфиденциальной компьютерной информации и специальных технических средств
103. Причинами низкой эффективности проектируемых БД могут быть:
a. + большая длительность процесса структурирования

b. + недостаточно глубокий анализ требований
c. - количество подготовленных документов
d. - скорость работы программных средств
e. - скорость заполнения таблиц
f. - скорость работы пользователя

104. Вирус возникает в ПК
a. + попадая извне с какими-либо программами
b. + при загрузке файлов из internet
c. - сам по себе
d. - при установке программ с лицензионных дисков
e. - от поддерживающей инфраструктуры
f. - от информации

105. Целостность можно подразделить
a. + статическую
b. + динамичную
c. - структурную
d. - графическую
e. - диафрагментнальную
f. - ломаную

106. Где применяются средства контроля динамической целостности
a. + анализе потока финансовых сообщений
b. + при выявлении кражи, дублирования отдельных сообщений
c. - обработке данных
d. - при отказе пользователей
e. - при отказе поддерживающей инфраструктуры
f. - в ошибках программ

107. Конфиденциальную информацию можно разделить
a. + предметную
b. + служебную
c. - глобальную
d. - случайные
e. - преднамеренные
f. - природные

108. Предпосылки появления угроз
a. + объективные
b. + субъективные
c. - преднамеренные
d. - случайные
e. - выборочные
f. – чередующеся

109. При помощи каких программ осуществляется отправка и получение электронной почты:
+ outlookexpress
+ the bat
Quicktime
Word
excel
powerpoint

110. Выберите действия, которые позволяют выполнять графические программы PAINT и PHOTOSHOP
+ редактировать графические файлы
+ создавать графические файлы

- создавать мелодии
- сохранять мелодии на диске в виде файлов
- редактировать мелодии

Контрольно-оценочные материалы для промежуточного контроля
Вопросы к экзамену
по учебной дисциплине «Основы информационной безопасности»

1. Понятие безопасности и защиты информации.
2. Понятие политики безопасности информационных систем. Назначение политики безопасности.
3. Основные типы политики безопасности доступа к данным.
4. Администрирование АИС: функции администратора, функции службы безопасности.
5. Механизмы безопасности, используемые для обеспечения "неотказуемости" системы
6. Администрирование средств безопасности
7. Виды избыточности в вычислительных сетях
8. Преимущества сети с выделенными каналами
9. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
10. Виды криптосистем.
11. Задачи, решаемые методами криптографии.
12. История криптографии. Основные этапы становления науки криптографии.
13. Методы криптографических преобразований.
14. Шифрование перестановкой.
15. Шифрование методом гаммирования и аналитического преобразования.
16. Многократное шифрование.
17. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров.
20. Идеальные шифры.
21. Идентификация и аутентификация при входе в информационную систему. Использование
22. парольных схем. Недостатки парольных схем.
23. Биометрические средства идентификации и аутентификации пользователей.
24. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
25. Законодательный уровень применения цифровой подписи.
26. Информационная сфера и ее элементы.
27. Понятие безопасности и информационной безопасности.
28. Основные составляющие информационной безопасности.
29. Субъекты и объекты правоотношений в области информационной безопасности.
30. Концептуальные положения организационного обеспечения информационной безопасности.
31. Понятие и виды угроз безопасности.
32. Угрозы информационной безопасности на объекте.
33. Организация службы безопасности объекта
34. Правовой режим информации: понятие, признаки, содержание.
35. Виды информации ограниченного доступа.
36. Требования, предъявляемые к организации защиты конфиденциальной информации.
37. Виды компьютерных преступлений.
38. Угрозы нарушения конфиденциальности, целостности, доступности информации.

39. Основные причины утечки информации.
40. Режим, правовой режим, правовой режим информации: определение.
41. Понятие правового режима информации и его основные признаки.
42. Понятие правового режима информации и его типовые элементы.
43. Характеристика видов правового режима информации с точки зрения его обязательности и объекта.
44. Общий правовой режим информации.
45. Специальные правовые режимы информации.
46. Тайна как специальный правовой режим.
47. Конфиденциальность как специальный правовой режим.
48. Государственная тайна и ее защита.
49. Угроза безопасности, обеспечение безопасности: понятие.
50. Информационная безопасность: понятие, первоочередные меры по обеспечению, общие методы.
51. Информационная безопасность и информационные войны: понятие.
52. Правонарушение и информационное правонарушение: определение, признаки, юридическая ответственность и основание привлечения к ответственности.
53. Состав информационного правонарушения.
54. Уголовная ответственность за информационное преступление.
55. Административная и гражданско-правовая ответственность в информационной сфере Защита персональных данных
56. Стратегия национальной безопасности РФ в информационной сфере.
57. Доктрина информационной безопасности РФ: назначение документа, источники угроз информационной безопасности РФ, общие методы обеспечения информационной безопасности РФ.
58. Нормативно-правовое регулирование защиты информации: направления защиты
59. Виды конфиденциальной информации: коммерческая тайна, персональные данные
60. Виды конфиденциальной информации: государственная служебная тайна, процессуальная тайна, авторское, патентное право.

Рекомендуемая литература

Основная литература :

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — URL : https://urait.ru/bcode/476997
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — URL : https://urait.ru/bcode/475889
3. Черткова, Е. А. Программная инженерия. Визуальное моделирование программных систем : учебник для среднего профессионального образования / Е. А. Черткова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 147 с. — (Профессиональное образование). — ISBN 978-5-534-09823-5. — URL : https://urait.ru/bcode/473307
4. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2022. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. —

Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497642

Дополнительная литература

1. Белов, П. Г. Системный анализ и программно-целевой менеджмент рисков : учебник и практикум для вузов / П. Г. Белов. — Москва : Издательство Юрайт, 2021. — 289 с. — (Высшее образование). — ISBN 978-5-534-04690-8. — URL : https://urait.ru/bcode/473132
2. Гниденко, И. Г. Технология разработки программного обеспечения : учебное пособие для среднего профессионального образования / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. — Москва : Издательство Юрайт, 2021. — 235 с. — (Профессиональное образование). — ISBN 978-5-534-05047-9. — URL : https://urait.ru/bcode/472502
3. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — URL : https://urait.ru/bcode/471382
4. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — URL : https://urait.ru/bcode/471910

Электронные ресурсы:

1. Открытые системы.- URL: http://biblioclub.ru/index.php?page=journal&jid=436083
2. Информатика в школе .- URL: http://dlib.eastview.com/browse/publication/18988
3. Программные продукты и системы.- URL: http://dlib.eastview.com/browse/publication/64086
2. Информатика и образование.- URL: http://dlib.eastview.com/browse/publication/18946
3. Системный администратор.- URL: http://dlib.eastview.com/browse/publication/66751
4. Computerword Россия.- URL: http://dlib.eastview.com/browse/publication/64081
   Мир ПК.- URL: http://dlib.eastview.com/browse/publication/64067
6. Информационно-управляющие системы.- URL: http://dlib.eastview.com/browse/publication/71235
7. Журнал сетевых решений LAN.- URL: http://dlib.eastview.com/browse/publication/64078
8. Информатика и образование.- URL: http://dlib.eastview.com/browse/publication/1894624
9. Прикладная информатика.- URL: http://elibrary.ru/title_about.asp?id=25599

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. ЭБС «Университетская библиотека ONLINE». – URL: www.biblioclub.ru
2. ЭБС издательства «Лань». – URL: https://e.lanbook.com
3. ЭБС «ZNANIUM.COM» www.znanium.com
4. Электронный каталог Научной библиотеки КубГУ. – URL:http://212.192.134.46/MegaPro/Catalog/Home/Index

5. Электронная библиотека «Издательского дома «Гребенников» - URL:www.grebennikon.ru
6. Научная электронная библиотека (НЭБ) «eLibrary.ru». - URL:http://www.elibrary.ru
7. Базы данных компании «Ист Вью». - URL:http://dlib.eastview.com
8. Лекториум ТВ». - URL: http://www.lektorium.tv/
9. Национальная электронная библиотека «НЭБ». - URL:http://нэб.рф/
10.КиберЛенинка: научная электронная библиотека. – URL: http://cyberleninka.ru/
10. Единое окно доступа к образовательным ресурсам : федеральная ИС свободного доступа. – URL: http://window.edu.ru.
11. Справочно-правовая система «Консультант Плюс» - URL http://www.consultant.ru