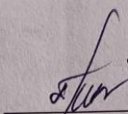


**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО  
ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Дагестанский государственный университет»  
*Колледж*

УТВЕРЖДАЮ

директор Колледжа

 Д.Ш. Пирбудагова

«14» 03 2022г.

Фонд оценочных средств  
по учебной дисциплине

**ОП.02 ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ  
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 2022 г.

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

Утверждена на заседании учебно-методического совета колледжа ДГУ

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

**ПАСПОРТ фонда оценочных средств  
по дисциплине**

**ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
1	Раздел I Информационные отношения и правовой режим защиты информации ограниченного доступа	ОК 01; ОК 02; ОК 03; ОК 04; ОК 06; ОК 09.	Подготовка рефератов; коллоквиум; тестирование; подготовка эссе.
2	Раздел II Правовая защита различных видов конфиденциальной информации и прав на результаты интеллектуальной	ПК 1.4; ПК 2.1; ПК 2.4; ПК 3.2; ПК 3.5	Подготовка рефератов; коллоквиум; тестирование; подготовка эссе.
3	Раздел III Организационное обеспечение информационной безопасности	ОК 06; ОК 09; ОК 03. ПК 1.4; ПК 2.1; 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 «Организационно-правовое обеспечение информационной безопасности»

№ п/п	Наименование оценочного средства	Критерии оценивания на «неудовлетворительно»	Критерии оценивания на «удовлетворительно»	Критерии оценивания на «хорошо»	Критерии оценивания на «отлично»
1	<b>Деловая и/или ролевая игра</b>	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	<b>Коллоквиум</b>	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	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.);	студент дает ответ, отличающийся меньшей обстоятельностью и глубиной изложения: обнаруживает при этом твердое 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

		наводящих вопросов.	испытывает существенные трудности при определении собственной оценочной позиции; наблюдается нарушение логики изложения материала.		; четко излагает материал в логической последовательности.
3	<b>Эссе</b>	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	<b>Тест</b>	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	<b>Лабораторная работа</b>	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 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	<b>Контрольная работа</b>	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, полнота обзора состояния вопроса; - обоснованность выводов.
7	<b>Реферат</b>	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. Используются 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	<b>Кейс-задача</b>	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	<b>Разнородные задачи и задания</b>	Неправильное решение задачи, отсутствие необходимых знаний теоретических аспектов решения казуса	Частично правильное решение задачи, недостаточная аргументация своего решения, определённое знание теоретических аспектов решения казуса, частичные ответы на дополнительные вопросы по теме занятия	Правильное решение задачи, достаточная аргументация своего решения, хорошее знание теоретических аспектов решения казуса, частичные ответы на дополнительные вопросы по теме занятия	Правильное решение задачи, подробная аргументация своего решения, хорошее знание теоретических аспектов решения казуса, ответы на дополнительные вопросы по теме занятия



Вопросы для коллоквиумов, собеседования  
по дисциплине «Организационно-правовое обеспечение информационной безопасности»

Раздел I. Информационные отношения и правовой режим защиты информации  
ограниченного доступа

1. Государство: понятие, признаки, функции
2. Формы государства
3. Правовое государство
4. Сущность права: признаки, структура, функции
5. Источники права
6. Норма права и система права
7. Понятие, предмет и объект гражданского права
8. Принципы гражданского права
9. Источники гражданского права
10. Объекты гражданского права
11. Субъекты гражданского права
12. Структура информационной сферы, характеристика ее элементов.
13. Информация как объект правоотношений, категории информации.
14. Система правовой защиты информации.
15. Понятие и виды защищаемой информации.
16. Особенности государственной тайны как защищаемой информации.
17. Система защиты государственной тайны.
18. Засекречивание информации, отнесенной к государственной тайне.
19. Защита сведений отнесенных к государственной тайне.
20. Понятие информации конфиденциального характера.
21. Основные виды конфиденциальной информации, в соответствии с требованиями российской нормативно-правовой базы.
22. Правовой режим конфиденциальной информации.
23. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
24. Понятие и характеристика служебной тайны.
25. Нормативно - правовые основы защиты служебной тайны.
26. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения.
27. Правовые основы защиты коммерческой тайны.
28. Виды информации, составляющей коммерческую тайну.
29. Права и обязанности обладателя коммерческой тайны.
30. Основные угрозы коммерческой тайны.
31. Правовая защита коммерческой тайны.
32. Правовые основы защиты банковской тайны.
33. Раскрытие информации, относящейся к банковской тайне.

Раздел II. Правовая защита различных видов конфиденциальной информации и прав на  
результаты интеллектуальной деятельности и средства индивидуализации.

1. Правовая защита результатов интеллектуальной деятельности.
2. Соотношение организационных мер защиты информации с мерами правового и технического характера.
3. Основные термины, связанные с организацией защиты информации.
4. Организационные меры, направленные на защиту государственной тайны.
5. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
6. Особенности системы организационной защиты государственной тайны.

7. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны.
8. Организация деятельности режимно-секретных органов.
9. Установление и изменение степени секретности сведений, отнесенных к государственной тайне.
10. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.
11. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы.
12. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
13. Документальное оформление для отправки на согласование.
14. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности.
15. Организация доступа к сведениям, составляющим государственную тайну.
16. Понятие «охрана». Цели и задачи охраны.
17. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны.
18. Виды, способы и особенности охраны различных объектов.
19. Понятие о рубежах охраны. Многорубежная система охраны.
20. Факторы выбора методов и средств охраны.
21. Организация охраны объектов защиты в процессе их транспортировки.
22. Понятие «режим», цели и задачи режимных мероприятий. Виды режима.
23. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков.

### Раздел III. Организационное обеспечение информационной безопасности

24. Виды пропускных документов.
25. Порядок организации работы бюро пропусков.
26. Контрольно-пропускные пункты, их оборудование и организация работы.
27. Понятие «внутриобъектовый режим» и его общие требования.
28. Противопожарный режим и его обеспечение.
29. Подбор и расстановка кадров.
30. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала.
31. Основные формы обучения и методы контроля знаний.
32. Мотивация персонала к выполнению требований по защите информации.
33. Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика.
34. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.
35. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
36. Организационные меры по защите информации при увольнении сотрудника.
37. Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров.
38. Основные этапы проведения конфиденциальных переговоров.
39. Подготовка помещения для проведения конфиденциальных переговоров.
40. Подготовка программы проведения конфиденциальных переговоров.
41. Порядок проведения конфиденциальных переговоров.
42. Требования режима защиты информации при приеме в организации

посетителей. Порядок доступа посетителей и командированных лиц к конфиденциальной информации. Порядок пребывания посетителей на территории и в помещениях организации.

43. Требования к программе приема иностранных представителей.
44. Требования к помещениям, в которых проводится прием иностранных представителей.
45. Обеспечение защиты информации при выезде за рубеж командированных лиц.
46. Основные виды и формы рекламы. Общие требования режима защиты информации в процессе рекламной деятельности.
47. Основные методы защиты информации в рекламной деятельности. Понятие «публикация в открытой печати». Общие требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.
48. Особенности защиты информации при опубликовании материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.
49. Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности.
50. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
51. Основные документы службы информационной безопасности

## **2.2. Контрольно-оценочные материалы для текущего контроля**

### **Тема 1.1. – Информационные отношения как объект правового регулирования.**

1. Законодательство Российской Федерации в области информационной безопасности.
2. Структура информационной сферы и характеристика ее элементов.
3. Информация как объект правоотношений.
4. Категории информации по условиям доступа к ней и распространения.
5. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
6. Субъекты и объекты правоотношений в области информационной безопасности.
7. Система нормативных правовых актов, регулирующие обеспечение информационной безопасности в Российской Федерации
8. Понятие и виды информации ограниченного доступа по законодательству РФ.

### **Тема 1.2.- Правовой режим защиты государственной тайны**

1. Понятие правового режима защиты государственной тайны.
2. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.
3. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
4. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

### **Тема 1.3.- Правовой режим защиты информации конфиденциального характера**

1. Понятие информации конфиденциального характера по российскому законодательству.
2. Основные виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства.
3. Правовой режим конфиденциальной информации: содержание и особенности.
4. Основные требования, предъявляемые к организации защиты конфиденциальной

информации

**Тема 2.1.-** Общая характеристика права интеллектуальной собственности как подотрасли гражданского права.

1. Теории интеллектуальной собственности.
2. Охраняемые результаты интеллектуальной собственности
3. Охраняемые средства индивидуализации.
4. Интеллектуальные права. Исключительное право

**Тема 2.2. –** Патентное право

1. Права авторов изобретения, полезной модели или промышленного образца. Объекты патентных прав.
2. Изобретение как объект патентных прав.
3. Условия патентоспособности изобретения.
4. Полезная модель как объект патентных прав.
5. Условия патентоспособности модели.
6. Промышленный образец как объект патентных прав. Условия патентоспособности промышленного образца.
7. Патентные права. Иные случаи ограничений исключительного права.
8. Сроки охраны исключительных прав.
9. Оформление патентных прав.
10. Особенности охраны служебных изобретений, полезных моделей, промышленных образцов.

**Тема 2.3. -** Институт правовой защиты служебной тайны

1. Правовые основы защиты служебной тайны.
2. Нормативно-правовые акты, регулирующие правовую защиту служебной тайны.
3. Защита в режиме служебной тайны сведений, доступ к которым ограничивается в соответствии с законодательством, при обращении и хранении таких сведений (информации) в органах государственной власти и органах местного самоуправления.
4. Защита служебной тайны в соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

**Тема 2.4. –** Институт правовой защиты банковской тайны

1. Правовые основы защиты банковской тайны.
2. Источники права о банковской тайне.
3. Объекты и субъекты права на банковскую тайну.
4. Права владельца банковской тайны в отношении сведений, составляющих его банковскую тайну.
5. Обязанности пользователей банковской тайны.

**Тема 2.5. -** Международно - правовая охрана интеллектуальной собственности

1. Основные международные соглашения в области авторского права.
2. Основные международные соглашения в области охраны смежных прав.
3. Основные международные соглашения в области охраны объектов патентного права, средств индивидуализации.
4. Иные международные соглашения в сфере интеллектуальной собственности.
5. Статус всемирной организации интеллектуальной собственности

### **Тема 3.1. - Понятие организационной защиты информации.**

1. Введение в организационное обеспечение информационной безопасности..
2. Сущность организационных методов защиты информации.
3. Основные термины, связанные с организацией защиты информации

### **Тема 3.2. - Организация режима секретности**

1. Организационные меры, направленные на защиту государственной тайны.
2. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
3. Порядок допуска и доступа к государственной тайне.
4. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
5. Понятие и особенности охраны.
6. Понятие «режим», цели и задачи режимных мероприятий.
7. Виды и организация пропускного режима.
8. Виды пропускных документов.
9. Направления и методы работы с персоналом, обладающим конфиденциальной информацией.
10. Организация обучения персонала.
11. Основные формы обучения и методы контроля знаний.
12. Мотивация персонала к выполнению требований по защите информации.

#### Самостоятельная работа № 1

##### **Информационные отношения как объект правового регулирования.**

1. Цифровое неравенство» и его влияние на другие формы неравенства;  
- перечень вопросов для самостоятельного изучения:
2. Государственное устройство Российской Федерации: официальные источники правовой информации
3. Нормативные правовые акты: официальное опубликование и вступление НПА в силу;
4. Федеральный регистр нормативных актов субъектов РФ

#### Самостоятельная работа № 2

##### **Правовой режим защиты государственной тайны**

1. Правовой режим защиты государственной тайны.
2. Правовой режим защиты информации конфиденциального характера.
3. Правовая защита персональных данных.
4. Государственное регулирование деятельности в области защиты информации

#### Самостоятельная работа № 3 **Правовой режим защиты информации конфиденциального характера**

1. Обнаружение загрузочного вируса
2. Характерные черты макровируса.
3. Наличие скрытых листов в Excel, как признак заражения макровирусом
4. Наиболее распространенные пути заражения компьютеров вирусами.
5. Особенности заражения компьютеров локальных сетей.
6. Ограничения заражения макровирусом при работе с офисными приложениями

Самостоятельная работа № 4 **Общая характеристика права интеллектуальной собственности как подотрасли гражданского права**

1. Система контроля за состоянием защиты государственной тайны
2. Перспективы развития законодательства в области информационной безопасности
3. Обязанности держателя профессиональной тайны. Защита доверителем своих прав
4. Практика расследования преступлений в сфере компьютерной информации
5. Возможность использования закона «О частной детективной и охранной деятельности» для правовой защиты персональных данных.

Самостоятельная работа № 5 **Патентное право**

1. Интеллектуальный шпионаж.
2. Особенности, виды, меры борьбы
3. Криминализация нарушений авторского и смежного права в Интернете

Самостоятельная работа № 6 **Институт правовой защиты служебной тайны**

1. Организационные меры, направленные на защиту государственной тайны
2. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны
3. Особенности системы организационной защиты государственной тайны
4. Распределение между уровнями государственного управления полномочий управленческих функций и задач по защите государственной тайны
5. Организация деятельности режимно-секретных органов.

Самостоятельная работа № 7 **Институт правовой защиты банковской тайны.**

1. Обязанности держателя профессиональной тайны.
2. Защита доверителем своих прав
3. Защита владельцем банковской тайны своих прав
4. Порядок восстановления нарушенных информационных прав
5. Права и обязанности органов государственной власти, иных государственных органов и органов местного самоуправления в отношении коммерческой тайны

Самостоятельная работа № 8 **Международно - правовая охрана интеллектуальной собственности**

1. Безопасность при транспортировке носителей информации
2. Порядок реализации режимных мер в ходе проведения выездных конфиденциальных переговоров
3. Обязанности лиц, участвующих в работе с иностранцами
4. Порядок выявления каналов утечки информации при организации публикационной деятельности
5. Режим защиты информации как составная часть организационной защиты информации

Самостоятельная работа № 9 **Понятие организационной защиты информации**

1. Организационные меры, направленные на защиту государственной тайны
2. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны
3. Особенности системы организационной защиты государственной тайны
4. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны,
5. Организация деятельности режимно-секретных органов



## Самостоятельная работа № 10 Организация режима секретности

1. Разновидности антивирусных программ
2. Защита информации от несанкционированного доступа
3. Безопасность и уязвимость в сети ИНТЕРНЕТ

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

#### по дисциплине

1. Организационно-правовое обеспечение информационной безопасности
2. Механизмы безопасности для обеспечения конфиденциальности трафика
3. Механизмы безопасности для обеспечения "неотказуемости" системы
4. Защита информации в персональном компьютере
5. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
6. Аудит в информационных системах.
7. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
8. Понятие электронной цифровой подписи.
9. Процедуры формирования цифровой подписи.
10. Единые критерии безопасности информационных технологий.
11. Понятие профиля защиты. Структура профиля защиты.
12. Единые критерии безопасности информационных технологий.
13. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
14. Административный уровень защиты информации.
15. Процедурный уровень обеспечения безопасности.
16. Авторизация пользователей в информационной системе.
17. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
18. Биометрические средства идентификации и аутентификации пользователей.
19. Криптографические методы защиты
20. Шифрование перестановкой.
21. Шифрование методом гаммирования и аналитического преобразования.
22. Классификация шифров замены. Шифр Цезаря.
23. Шифр простой замены.
24. Шифр Хилла. Шифр Виженера.
25. Частотный анализ.
26. Стандарты шифрования.
27. Режимы шифрования.
28. Многократное шифрование.
29. Композиция блочных шифров.
30. Совершенные шифры. Пример совершенного шифра.
31. Энтропийные характеристики шифров.
32. Идеальные шифры.
33. Избыточность языка.
34. Стандарт шифрования DES, Стандарт шифрования RSA.
35. Борьба с вирусным заражением информации
36. Правовое обеспечение защиты информации
37. Структура современных вирусов.
38. Защита от воздействия вирусов
39. Международные, российские и отраслевые правовые документы.
40. Концепция правового обеспечения информационной безопасности РФ.

41. Международные правовые акты по защите информации.
42. Федеральный закон «Об информации, информационных технологиях и о защите информации»

Темы эссе  
(рефератов, докладов, сообщений)

1. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
2. Административный уровень защиты информации.
3. Процедурный уровень обеспечения безопасности.
4. Авторизация пользователей в информационной системе.
5. Биометрические средства идентификации и аутентификации пользователей.
6. Криптографические методы защиты
7. Шифрование перестановкой.
8. Шифрование методом гаммирования и аналитического преобразования.
9. Классификация шифров замены. Шифр Цезаря.
10. Шифр простой замены.
11. Шифр Хилла. Шифр Виженера.
12. Частотный анализ.
13. Стандарты шифрования.
14. Режимы шифрования.
15. Многократное шифрование.
16. Совершенные шифры. Пример совершенного шифра.
17. Энтропийные характеристики шифров.
18. Эдеальные шифры.
19. Международные, российские и отраслевые правовые документы.
20. Концепция правового обеспечения информационной безопасности РФ.
21. Международные правовые акты по защите информации.

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

**Тема 1.1. – Информационные отношения как объект правового регулирования**

1. Термином «право» обозначается:
  - а) обоснованная, оправданная свобода или возможность поведения человека в его взаимоотношениях с другими людьми, которая признана и поддерживается обществом;
  - б) отрасль науки, которая изучает уголовный кодекс;
  - в) отрасль науки, которая изучает уголовный кодекс;
  - г) нет верного ответа.
2. В зависимости от формы проявления общественного признания этой свободы и способа ее поддержки со стороны общества различают следующие виды права:
  - а) обычное право, моральное право, корпоративное право;
  - б) обычное право, моральное право, корпоративное право, естественное право, юридическое право;
  - в) естественное право, юридическое право;
  - г) корпоративное право, естественное право.
3. Юридическое право представляет собой:
  - а) систему общеобязательных норм, выраженных в только в уставах организаций;
  - б) свободу, или возможность поведения, основанную на принципах добра, справедливости (заботливое отношение детей к родителям, уважение к женщине);
  - в) свободу, или возможность поведения, основанную на уставных и иных положениях, которые действуют внутри общественных, негосударственных объединений, организаций, партий (право избирать и быть избранным в руководящие органы, право руководящих органов налагать взыскания);
  - г) систему общеобязательных норм, выраженных в законах, иных признаваемых государством источниках права и являющихся общеобязательным основанием для определения правомерно-дозволенного, запрещенного и предписанного поведения

4. Наиболее известными в настоящее время правовыми системами являются:
- а) религиозная, базирующаяся на священной для мусульман книге — Коране (мусульманское право характерно, например, для Ирана);
  - б) романо-германская, основанная на праве законодателя (континентальная Европа);
  - в) прецедентная, основанная на праве судей (Великобритания и США);
  - г) верны все варианты.
5. Предмет правового обеспечения информационной безопасности представляет собой:
- а) совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз;
  - б) совокупность общественных отношений, на которые направлено правовое воздействие только в целях недопущения проявлений угроз объектам национальных интересов в информационной сфере;
  - в) нет верного ответа.
6. Правовое обеспечение безопасности информации в форме сведений образуется:
- а) совокупностью норм и институтов, регулирующих отношения по поводу только объекта - сведений, обладателем которых является субъект права;
  - б) совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права;
  - в) свобода мысли; субъективная значимость национальных культурных ценностей;
  - г) совокупностью норм и институтов, регулирующих отношения по поводу только объекта - свобода мысли.
7. Правовое обеспечение безопасности информации в форме сообщений определяется:
- а) совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей;
  - б) совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются сообщения, передаваемые по каналам связи, данные, накапливаемые и обрабатываемые в информационных системах, автоматизированных системах управления, а также документы как входящие, так и не входящие в информационные системы;
  - в) совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются средства связи, автоматизации обработки информации, информационно-телекоммуникационные системы и средства массовой информации;
  - г) совокупностью правовых норм и институтов.
8. Содержание и структура законодательства в области информационной безопасности включает:
- а) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации - Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;
  - б) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации;
  - в) Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;
  - г) нет верного ответа.
9. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации состоит из:
- а) Федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения в области использования информации;
  - б) Федерального закона «О персональных данных» и других федеральных законов, регулирующих отношения в области использования информации;
  - в) Федерального закона «О коммерческой тайне» и других федеральных законов, регулирующих отношения в области использования информации;
  - г) Федерального закона «О государственной тайне» и других федеральных законов, регулирующих отношения в области использования информации.
10. Предметом правового регулирования в области информации, информационных технологий и защиты информации являются:
- а) отношения, возникающие только при осуществлении права на поиск, получение, передачу, производство и распространение информации;
  - б) отношения, возникающие только при применении информационных технологий;
  - в) отношения, возникающие только при обеспечении защиты информации;
  - г) отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации.
11. Документированной информацией называют:
- а) Информацию, зафиксированную на материальном носителе путем документирования, с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

- б) Информацию, зафиксированную на материальном носителе путем документирования, без реквизитов;  
в) нет верного ответа.
12. К общедоступной информации относятся:
- а) общеизвестные сведения и иная информация, доступ к которой не ограничен после достижения определенного возраста;  
б) общеизвестные сведения и иная информация, доступ к которой не ограничен;  
в) нет верного ответа.
13. Различают следующие виды информационных систем:
- а) государственные информационные системы, муниципальные информационные системы, иные информационные системы;  
б) государственные информационные системы;  
в) муниципальные информационные системы;  
г) нет верного ответа.
14. Правовой режим информационных технологий включает:
- а) порядок регулирования использования информационно коммуникационных сетей;  
б) перечень областей государственного регулирования в сфере применения информационных технологий;  
в) требования к государственным информационным системам;  
г) верны все варианты.

### **Тема 1.2.- Правовой режим защиты государственной тайны**

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:
- а) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;  
б) соблюдение конфиденциальности информации ограниченного доступа;  
в) реализацию права на доступ к информации;  
г) верны все варианты.
2. В структуру государственной системы защиты информации РФ входят:
- а) ФСБ РФ;  
б) МВД РФ;  
в) ФСТЭК;  
г) ФСИН
3. Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:
- а) отнесенные к государственной тайне;  
б) отнесенные к служебной тайне (информации для служебного пользования), персональные данные (и другие виды тайн);  
в) отнесенные к информации о прогнозах погоды;  
г) все верны ответы.
4. Как называется закон, регулирующий деятельность государственной тайны на территории РФ?
- а) «О коммерческой тайне»;  
б) «О государственной тайне»;  
в) «О служебной тайне»;  
г) «О врачебной тайне».
5. Нормативно-правовой акт - это:
- а) правовой акт, принятый полномочным на то органом и содержащий правовые нормы, т. е. предписания общего характера и постоянного действия, рассчитанные на многократное применение;  
б) правовой акт, принятый полномочным на то органом и содержащий правовые нормы, т. е. предписания общего характера и постоянного действия, рассчитанные на однократное применение;  
в) нет верного ответа.
6. К информации ограниченного доступа относятся:
- а) государственная тайна;  
б) конфиденциальная информация;  
в) персональные данные;  
г) все ответы верны.
7. Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:
- а) отнесенные к государственной тайне;  
б) отнесенные к служебной тайне (информации для служебного пользования), персональные данные (и другие виды тайн);

- в) отнесенные к информации о прогнозах погоды;
- г) все верны ответы.
8. Государственная тайна — это:
- а) защищаемые государственные сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;
- б) защищаемые государственные сведения только в области военной и внешнеполитической деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;
- в) защищаемые государственные сведения только в области экономической и разведывательной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации.
9. К информации ограниченного доступа относятся:
- а) государственная тайна;
- б) конфиденциальная информация;
- в) персональные данные;
- г) все ответы верны.
10. Государственная тайна — это:
- а) информация, сведения, несанкционированный доступ к которым может причинить вред интересам страны, государства;
- б) информация, сведения, несанкционированный доступ к которым может причинить вред интересам только жителям страны, но всего государства;
- в) информация, сведения, несанкционированный доступ к которым может причинить вред интересам только руководству страны, государства.
11. Как называется закон, регулирующий деятельность государственной тайны на территории РФ?
- а) «О коммерческой тайне»;
- б) «О государственной тайне»;
- в) «О служебной тайне»;
- г) «О врачебной тайне».
6. Назовите признаки государственной тайны?
- а) это очень важные сведения; их разглашение может причинить ущерб государственным интересам; перечень сведений, которые могут быть отнесены к государственной тайне, закрепляется федеральным законом;
- б) это очень важные сведения и их разглашение может причинить ущерб государственным интересам;
- в) это очень важные сведения и перечень сведений, которые могут быть отнесены к государственной тайне, закрепляется федеральным законом.
12. К носителям сведений, составляющих государственную тайну относятся:
- а) материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отражение в виде символов, образов, сигналов, технических решений и процессов;
- б) материальные объекты, за исключением физических полей, в которых сведения, составляющие государственную тайну, находят свое отражение в виде символов, образов, сигналов, технических решений и процессов;
- в) нет верного ответа.
13. Гриф секретности — это:
- а) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе кроме сопроводительной документации на него;
- б) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.
- в) оба варианта верны.
14. Степень секретности — это:
- а) категория, характеризующая важность такой информации, возможный ущерб в случае ее разглашения, степень ограничения доступа к ней и уровень ее охраны государством;
- б) категория, характеризующая важность такой информации, возможный ущерб в случае ее разглашения, но не степень ограничения доступа к ней и уровень ее охраны государством;
- в) нет верного ответа.

### **Тема 1.3.- Правовой режим защиты информации конфиденциального характера**

1. Устанавливаются степени секретности сведений, составляющих государственную тайну:
- а) три;
- б) две;
- в) четыре.

2. Субъектами отнесения сведений к государственной тайне являются:
- а) Палаты Федерального Собрания;
  - б) Президент Российской Федерации;
  - в) Правительство Российской Федерации;
  - г) Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий;
  - д) верны все варианты.
3. Не подлежат отнесению к государственной тайне и засекречиванию сведения:
- а) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
  - б) состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
  - в) размерах золотого запаса и государственных валютных резервах Российской Федерации;
  - г) верны все варианты.
4. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать:
- а) 30 лет;
  - б) 40 лет;
  - в) 50 лет;
  - г) 60 лет.
5. Персональные данные - это:
- а) конкретная информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);
  - б) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);
  - в) любая информация, относящаяся к определенному или определяемому на основании такой информации юридическому лицу (субъекту персональных данных).
6. Субъект персональных данных обладает правами:
- а) на доступ к своим персональным данным;
  - б) возражение против принятия решений исключительно на основании автоматизированной обработки персоналом данных, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы;
  - в) обжалование действий или бездействий;
  - г) верны все варианты
7. ИСПДн согласно 5 пункту Постановления №1119 подразделяются на следующие группы (категории):
- а) Специальные ИСПДн;
  - б) Биометрические ИСПДн;
  - в) Общедоступные ИСПДн;
  - г) Иные ИСПДн;
  - д) верны все варианты.
8. По форме отношений между организацией и субъектами, обработка подразделяется на следующие виды:
- а) обработка ПДн сотрудников (субъектов, с которыми организация связана трудовыми отношениями);
  - б) обработка ПДн субъектов, не являющихся сотрудниками организации;
  - в) верны оба варианта.
9. По количеству субъектов ПДн определены только следующие категории:
- а) менее 100 000 субъектов;
  - б) более 100 000 субъектов;
  - в) верны оба варианта.
10. По типу актуальных угроз ИСПДн подразделяются на:
- а) угрозы 1-го типа связанные с наличием недекларированных (недокументированных) возможностей в системном ПО (операционная система), используемом в ИСПДн;
  - б) угрозы 2-го типа связанные с наличием недекларированных возможностей в прикладном ПО (программы обработки ПДн), используемом в ИСПДн;
  - в) угрозы 3-го типа не связанные с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн;
  - г) верны все варианты.
11. Требованиями к защите ПДн при их обработке в информационных системах (Утв. Постановлением Правительства № 1119 от 01.11.2012) установлены следующие уровни защищенности персональных данных:
- а) УЗ-1 - максимальный уровень защищенности ПДн;
  - б) УЗ-2 - высокий уровень защищенности ПДн;
  - в) УЗ-3 - средний уровень защищенности ПДн;



- г) УЗ-4 - низкий уровень защищенности ПДн;
- д) верны все варианты.

### **Тема 2.1.- Общая характеристика права интеллектуальной собственности как подотрасли гражданского права**

1. Официальный документ, занимающий главное место в системе законодательства в области авторского права РФ
  - а) Конституция РФ;
  - б) Уголовный Кодекс РФ;
  - в) Гражданский Кодекс;
  - г) Трудовой Кодекс.
2. 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".
3. 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.
4. 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.
5. 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.
6. 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%.
7. 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.
8. 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.
9. 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 варианта.
10. 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.
11. 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.

## **Тема 2.2. – Патентное право**

1. 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.
2. 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.
3. На документах, предоставляемых указанным органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф:
- а) «Коммерческая тайна»;
  - б) «Служебная тайна»;
  - в) «Деловая тайна».
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. Из скольких уровней состоит правовое обеспечение информационной безопасности:
- а) двухуровневой;
- б) трех уровней;
- в) четырех уровней;
- г) пяти уровней.
10. Правовой режим объекта правоотношения может быть:
- а) **общим**
- б) **специальным**
- в) открытым
- г) ограниченным
11. Правовой режим объекта правоотношения может быть:
- а) **общим**
- б) **специальным**
- в) императивным
- г) диспозитивным
12. В главе 19 УК «Преступления против конституционных прав и свобод человека и гражданина» предусмотрена ответственность за информационные преступления
- а) **отказ в предоставлении гражданину информации**
- б) **нарушение авторских и смежных прав**
- в) разглашение информации с ограниченным доступом
- г) нарушение правил распространения обязательных сообщений
13. Виды ответственности юридических лиц за информационные правонарушения:
- а) **административная**
- б) **гражданско-правовая**
- в) дисциплинарная
- г) уголовная

### Тема 2.3. - Институт правовой защиты служебной тайны

1. Как называется стандарт ГОСТ Р ИСО/МЭК 15408-1—2002?
- а) Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
- 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.
2. Как называется стандарт ГОСТ Р 50739-95?
- а) Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
- 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.
3. Как называется стандарт ГОСТ Р 50922-96?
- а) Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
- 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.
4. Как называется стандарт ГОСТ Р ИСО 7498-2-99?
- а) Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
- 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.
5. 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.
6. 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.
7. 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 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
- г) ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

#### **Тема 2.4. – Институт правовой защиты банковской тайны**

1. Информацию по степени доступа разделяют на:
- а) открытую и ограниченного доступа;
- б) открытую;
- в) закрытую;
- г) тайную и ограниченную.
2. К информации ограниченного доступа относятся:
- а) государственная тайна;
- б) конфиденциальная информация;
- в) персональные данные;
- г) все ответы верны.
3. Информационная безопасность являются переводом на русский язык английского термина:
- а) informationsecurity;
- б) informationsystem;
- в) informationcurrency;
- г) informationcrypto.
4. 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.
5. Под утечкой понимают:
- а) неконтролируемое распространение защищаемой информации путем ее разглашения или несанкционированного доступа к ней;
  - б) неконтролируемое распространение скрытой информации путем её разглашения или несанкционированного доступа к ней;
  - в) неконтролируемое распространение конфиденциальной информации путем ее разглашения или несанкционированного доступа к ней;
  - г) все верно.
6. Под непреднамеренным воздействием на защищаемую информацию понимают:
- а) воздействие на неё из-за ошибок пользователя, сбоя технических или программных средств, иных нецеленаправленных действий;
  - б) воздействие на неё из-за ошибок пользователя, сбоя технических средств;
  - в) воздействие на неё из-за ошибок пользователя, программных средств, иных нецеленаправленных действий;
  - г) все ответы верны.
7. Что не является характеристикой информации:
- а) статичность;
  - б) тип доступа;
  - в) время отклика;
  - г) стоимость создания.
8. К наиболее распространённым 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.
9. Что не относится к задачам информационной безопасности:
- а) целостность и секретность;
  - б) электронная подпись и датирование;
  - в) устойчивость связи и определение трафика;
  - г) анонимность.
10. К методам обеспечения информационной безопасности не относятся:
- а) корпоративные;
  - б) административные;
  - в) правовые;
  - г) технические.
11. 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.
12. 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.
13. Метод физического преграждения пути злоумышленнику к информации:
- а) управление доступом;
  - б) маскировка;
  - в) принуждение;
  - г) побуждение.

## **Тема 2.5. - Международно - правовая охрана интеллектуальной собственности**

1. К методам обеспечения информационной безопасности не относятся:
- а) корпоративные;
  - б) административные;
  - в) правовые;
  - г) технические.
2. 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.
3. 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.
4. Методы, не имеющие математического обоснования стойкости, часто называют методами:
- а) С чёрным ящиком;
  - б) С белым квадратом;
  - в) С желтым кругом;
  - г) Нет верного ответа.
5. Методы, функционирующие по принципу "черного ящика", называют
- а) SecurityThroughObscurity;
  - б) System ThroughObscurity;
  - в) SecurityThrough;
  - г) SystemObscurity.
6. Метод физического преграждения пути злоумышленнику к информации:
- а) управление доступом;
  - б) маскировка;
  - в) принуждение;
  - г) побуждение.
7. Метод защиты информации путем ее криптографического преобразования:
- а) Принуждение;
  - б) Побуждение;
  - в) Маскировка;
  - г) управление доступом.
8. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:
- а) Уполномочивание;
  - б) Контроль доступа;
  - в) Сертификация;
  - г) Нет верного ответа.
9. 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.
10. 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.
11. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:
- а) статичность;
  - б) атака;
  - в) угроза;
  - г) изъясн.
12. 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
13. К каналам, предполагающим изменение элементов информационной структуры относится:
- а) намеренное копирование файлов и носителей информации;
  - б) маскировка под других пользователей, путём похищение идентифицирующей их информации;
  - в) хищение носителей информации;
  - г) незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.
14. 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.
15. 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.
16. К какому типу атак относится прослушивание передаваемых сообщений:
- а) Пассивная атака;
  - б) Модификация потока данных;
  - в) Повторное использование;
  - г) Отказ в обслуживании.
17. 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.
18. Метод защиты информации путем ее криптографического преобразования:
- а) Принуждение;
  - б) Побуждение;
  - в) Маскировка;
  - г) управление доступом.
19. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:
- а) Уполномочивание;
  - б) Контроль доступа;
  - в) Сертификация;
  - г) Нет верного ответа.
20. 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.

### **Тема 3.1. - Понятие организационной защиты информации.**

1. Режим секретности – это:
- а) совокупность определяемых органами власти и управления правил, которыми ограничивается допуск лиц к секретным материалам и работам, регламентируется порядок пользования секретных материалов, соответствующим образом регулируется поведение людей, имеющих отношение к секретам, и предусматриваются другие меры;
  - б) совокупность определяемых органами власти и управления правил, по которым лица имеют неограниченный допуск к секретным материалам и работам, регламентируется порядок пользования секретных материалов, соответствующим образом регулируется поведение людей, имеющих отношение к секретам, и предусматриваются другие меры;
  - в) нет верного ответа;
2. Назначение режима секретности заключается, в том, чтобы:
- а) ограничить сферу обращения секретных данных только кругом лиц, связанных с производством секретных работ;
  - б) ограничить сферу обращения секретных данных всех лиц, имеющих доступ к какой-либо информации;
  - в) ограничить частично сферу обращения секретных данных только кругом лиц, связанных с производством секретных работ;
3. Назовите главные элементы режима секретности?
- а) правила засекречивания; рассекречивания; защита государственной тайны;
  - б) правила засекречивания и защита государственной тайны;
  - в) правила засекречивания и рассекречивания;

- г) защита государственной тайны и рассекречивания;
4. Не подлежат засекречиванию сведения о:
- а) чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях;
  - б) сведения о военных разработках;
  - в) сведения о технических разработках;
5. Что такое аудит?
- а) анализ накопленной информации, проводимый только оперативно;
  - б) анализ накопленной информации, проводимый оперативно или периодически;
  - в) оба ответа верны;
6. Выработку политики безопасности и ее содержание рассматривают на \_\_\_\_ горизонтальных уровнях детализации?
- а) трех;
  - б) двух;
  - в) четырех;
7. Наибольшую угрозу ИС составляют:
- а) Юзер;
  - б) Агент;
  - в) Хакер;
  - г) Крякер;
8. Внутриобъектовый режим это?
- а) комплекс мероприятий, направленных на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия;
  - б) Только 1 мероприятие, направленное на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия;
  - в) нет верного ответа;
9. 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.
10. Пропускной режим — это?
- а) совокупность норм и правил, регламентирующих порядок входа на территорию предприятия и выхода лиц, въезда и выезда транспортных средств, вноса и выноса, ввоза и вывоза носителей сведений конфиденциального характера, а также мероприятий по реализации названных норм и правил с использованием имеющихся сил и средств;
  - б) совокупность норм и правил, регламентирующих порядок выхода из территории предприятия, выезда транспортных средств, вноса и выноса, ввоза и вывоза носителей сведений конфиденциального характера, а также мероприятий по реализации названных норм и правил с использованием имеющихся сил и средств
  - в) нет верного ответа
11. 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;
12. 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.
13. К какому типу атак относится прослушивание передаваемых сообщений:
- а) Пассивная атака;
  - б) Модификация потока данных;
  - в) Повторное использование;
  - г) Отказ в обслуживании.
14. В номенклатуру современных технических средств и аксессуаров для оперативно-розыскных мероприятий входят:
- а) средства оперативной связи;
  - б) системы поиска и слежения за подвижными объектами;
  - в) средства негласного доступа в помещения;
  - г) средства маркирования объектов;
  - д) все верны варианты.

15. В номенклатуру современных технических средств и аксессуаров для оперативно-розыскных мероприятий входят:

- а) программные средства;
- б) штурмовое оборудование;
- в) системы подавления радиосредств, средства радио мониторинга, системы пеленгации;
- г) коммутаторы, телефонные станции с автоматическим определением номера;
- д) все верны варианты.

16. В номенклатуру современных технических средств и аксессуаров для оперативно-розыскных мероприятий входят:

- а) средства обнаружения радиоактивных материалов, взрывчатых и химических веществ;
- б) рентгеноскопическое оборудование;
- в) обнаружители оружия;
- г) роботизированные комплексы;
- д) все верны варианты.

17. Примером нарушения статической целостности не является:

- а) ввод неверных данных;
- б) несанкционированное изменение данных;
- в) изменение программного модуля вирусом;
- г) внесение дополнительных пакетов в сетевой трафик;

18. Организация режима секретности включает проведение следующих процедур:

- а) засекречивание (рассекречивание) путем установления степени секретности сведений, содержащихся в документах, используемых или создаваемых на режимном объекте;
- б) оформление допуска, т.е. особых видов документов, подтверждающих наличие у сотрудника санкции на работу с документами, содержащими государственную тайну;
- в) контроль выполнения должностными лицами установленных правил работы с секретными документами;
- г) верны все варианты.

19. Преступлениями в сфере компьютерной информации на территории РФ являются:

- а) Неправомерный доступ к компьютерной информации (ст.272 УК РФ);
- б) Создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ);
- в) Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ);
- г) верны все варианты.

20. Субъектом преступления, указанного в ч. 1 ст. 272, может быть любое вменяемое физическое лицо, достигшее:

- а) 16 лет;
- б) 18 лет;
- в) 14 лет;
- г) 21 года

### Тема 3.2. - Организация режима секретности

1. Что такое лицензирование?

- а) это процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ;
- б) это процесс передачи, но не получения в отношении физических или юридических лиц прав на проведение определенных работ;
- в) это процесс получения, но не передачи в отношении физических или юридических лиц прав на проведение определенных работ.

2. Что такое лицензия?

- а) документ, дающий право на осуществление указанного вида деятельности в течение неограниченного времени;
- б) документ, дающий право на осуществление указанного вида деятельности в течение определенного времени;
- в) документ, дающий право на осуществление любого вида деятельности в течение неограниченного времени.

3. Перечень видов деятельности в области защиты информации, на которые выдаются лицензии, определен Постановлением Правительства РФ - «О лицензировании отдельных видов деятельности» от 24.12.94 №1418 к ним, в частности, относится разработка, производство, реализация и сервисное обслуживание:

- а) шифровальных средств;
- б) защищенных систем телекоммуникаций;
- в) программных средств;

г) специальных технических средств защиты информации;

д) подготовка и переподготовка кадров;

е) все верны варианты.

4. Что такое сертификация?

а) подтверждение соответствия продукции или услуг установленным требованиям или стандартам;

б) подтверждение соответствия продукции, но не услуг установленным требованиям или стандартам;

в) подтверждение соответствия услуг, но не продукции установленным требованиям или стандартам.

5. Что такое сертификат?

а) документ, подтверждающий соответствие средства защиты информации требованиям по безопасности информации;

б) документ, подтверждающий соответствие средства защиты информации требованиям по хранению информации;

в) документ, подтверждающий соответствие средства защиты информации требованиям по обработке информации.

6. Законодательной и нормативной базой лицензирования и сертификации в области защиты информации являются законы РФ:

а) —О государственной тайне<sup>1</sup> от 21.07.93 №5485-1;

б) —О техническом регулировании<sup>1</sup> от 27 декабря 2002 г. N 184-ФЗ;

в) —О лицензировании отдельных видов деятельности<sup>1</sup>, от 8.08 2001г.

№128 (ред. от 11.03.2003г. №32);

г) —О защите прав потребителей<sup>1</sup> от 07.02.92 №2300-1;

д) все верны варианты.

7. Законодательной и нормативной базой лицензирования и сертификации в области защиты информации являются законы РФ:

а) —О лицензировании отдельных видов деятельности<sup>1</sup> от 24 12 94

№1418;

б) —О лицензировании деятельности предприятий...<sup>1</sup> от 15.04.95 №333;

в) —О сертификации средств защиты информации<sup>1</sup> от 26.06.95 №608.

г) —О лицензировании... от 27.05.2002 №348.

д) —О лицензировании... от 30.04.2002 №290, (ред. №64 от 6.02.2003).

е) все верны варианты.

8. Лицензированию подлежат следующие виды работ и услуг, контролирующие защищенность конфиденциальной информации от утечки по техническим каналам в:

а) средствах и системах информатизации;

б) технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

в) помещениях со средствами (системами), подлежащими защите;

г) помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);

д) все верны варианты верны.

9. Лицензированию подлежат следующие виды работ и услуг, контролирующие защищенность конфиденциальной информации от утечки по техническим каналам в:

а) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

б) помещений со средствами (системами) информатизации, подлежащими защите;

в) сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации (далее – СЗИ), защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации);

г) все верны варианты.

10. Какой номер имеет положение о сертификации средств защиты информации, утвержденного постановлением Правительства Российской Федерации от 25.06.95 г?

а) № 608;

б) № 607;

в) № 606;

г) № 609.

11. Назовите принципы сертификации:

а) сертификация изделий, обеспечивающих защиту ГТ, является обязательной;

б) обязательность использования криптографических алгоритмов, являющихся стандартами;

в) принятие на сертификацию изделий только от заявителей, имеющих лицензию;

г) все верны варианты.

12. На какой срок выдается сертификат?

а) до 4 лет;

б) до 3 лет;

в) до 5 лет;

г) до 6 лет.

13. Комплексный аудит информационной безопасности включает в себя следующие виды услуг:

а) анализ защищенности внешнего периметра корпоративной сети;

б) анализ защищенности внутренней ИТ-инфраструктуры;

в) оценка соответствия международному стандарту ISO 27001;

г) все верны варианты.

14. Комплексный аудит информационной безопасности включает в себя следующие виды услуг:

а) оценка соответствия требованиям законодательства и нормативной базы РФ в области защиты информации;

б) аудит безопасности критичных бизнес приложений;

в) все верны варианты.

15. Анализ защищенности внутренней ИТ-инфраструктуры организации предполагает проведение полного комплекса мероприятий по техническому аудиту, включая:

а) анализ конфигурационных файлов маршрутизаторов, МЭ, почтовых серверов, DNS серверов и других критичных элементов сетевой инфраструктуры;

б) анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств и списков проверки;

в) сканирование хостов, входящих в состав ЛВС;

г) все верны варианты.

16. Эффективность менеджмента в области информационной безопасности зависит от таких факторов:

а) - уровень, прогрессивности технических решений по обеспечению безопасности информации, применяемых на предприятии;

б) - выполнение положений законодательства и корпоративных нормативных актов в области обеспечения безопасности информации;

в) - качество персонала предприятия, характеризуемого прежде всего его лояльностью и квалификацией;

г) верны все варианты.

17. При подборе и расстановке кадров в области обеспечения информационной безопасности предприятия в первую очередь проводятся специальные мероприятия:

а) - учет вопросов конфиденциальности в традиционных кадровых методиках и процедурах приема и увольнения;

б) - подготовка нормативно-правовой базы по документированию добровольного согласия работника на определенное ограничение прав, связанное с дополнительным контролем его деятельности в целях обеспечения безопасности предприятия;

в) верны оба варианта.

18. Важным направлением деятельности по обеспечению информационной безопасности является подготовка кадров, которую проводят:

а) образовательные учреждения федеральных органов исполнительной власти, решающие в основном традиционные задачи защиты информации, в первую очередь, от внешних угроз;

б) - образовательные учреждения Минобрнауки России, осуществляющие подготовку специалистов по широкому кругу вопросов создания защищенных информационных систем, а также технических и программных средств защиты информации;

в) - негосударственные образовательные учреждения, в том числе региональные;

г) верны все варианты.

19. Перечень видов деятельности в области защиты информации, на которые выдаются лицензии, определен Постановлением Правительства РФ —О лицензировании отдельных видов деятельности<sup>1</sup> от 24.12.94 №1418 к ним, в частности, относится разработка, производство, реализация и сервисное обслуживание:

а) - шифровальных средств;

б) - защищенных систем телекоммуникаций;

в) - программных средств;

г) - специальных технических средств защиты информации;

д) верны все варианты.

20. Законодательной и нормативной базой лицензирования и сертификации в области защиты информации являются законы РФ:

а) -"О государственной тайне" от 21.07.93 №5485-1;

б) -"О техническом регулировании" от 27 декабря 2002 г. N 184-ФЗ;

в) -"О лицензировании отдельных видов деятельности", от 8.08 2001г. №128

(ред. от 11.03.2003г. №32);

г) верны все варианты.

## **Деловые игры**

### **«Построение модели угроз информационной безопасности для малого предприятия»**

Цель деловой игры: Анализ эффективности системы информационной безопасности (ИБ) организации с использованием аппарата моделирования с полным перекрытием множества угроз (программный инструментарий прилагается) с привлечением Специалистов отдела ИТ, Специалистов отдела защиты информации и Экспертов-аналитиков по ИБ.

Роли участников игры:

Специалисты отдела ИТ (3-4 человека)

При проектировании или оценки эффективности существующей системы защиты информации, чрезвычайно важно, чтобы различные конфликтные ситуации между сотрудниками службы ИТ и специалистами отдела защиты информации разрешались в форме продуктивного диалога.

Задачи специалистов отдела ИТ в данной деловой игре.

1. Подготовить для специалистов отдела защиты информации материалы по потенциальным угрозам ИБ, перечню инцидентов ИБ и прочие материалы, необходимые для анализа и построения модели ИБ в организации. Для достижения поставленной цели специалисты отдела ИТ должны проанализировать структуру объекта оценки и подготовить ответы на вопросы для специалистов отдела защиты информации и экспертов-аналитиков.

2. Провести совместное совещание со специалистами отдела защиты информации (ЗИ) с целью анализа ответов на вопросы информирования полного множества угроз; множества объектов защиты; множества средств защиты информации, имеющихся в данной организации.

3. Принять участие в итоговом совещании всех специалистов с целью анализа эффективности существующей системы защиты информации в организации и выработке рекомендаций по ее усовершенствованию.

Специалисты отдела защиты информации(3-4 человека)

Одной из задач специалистов по защите информации является оценка эффективности существующей в организации системы ИБ. Для решения этой задачи необходимо проводить интервью со специалистами ИТ с целью выявления слабостей в системе защиты информации, анализа инцидентов ИБ и подготовки материалов для построения модели: угрозы-средства защиты-объекты оценки.

Задачи специалистов отдела ЗИ в данной деловой игре.

1. Запросить у специалистов ИТ опросники, помочь в заполнении опросников и проконсультировать ИТ-специалистов в случае возникновения неоднозначных ситуаций.

2. Проанализировать полученные из отдела ИТ опросники (внести дополнительные сведения, при необходимости). На основании изучения описания организации и опросника, полученного от специалистов ИТ, заполнить формы анализа угроз ИБ для передачи экспертам-аналитикам.

3. Провести совместное совещание со специалистами отдела ИТ с целью формирования множества угроз; множества объектов защиты; множества средств защиты информации, имеющихся в данной организации.

4. Передать скорректированные тексты экспертам-аналитикам и внести сведения в базу данных.

5. Принять участие в итоговом совещании всех специалистов с целью анализа эффективности существующей системы защиты информации в организации и выработке рекомендаций по ее усовершенствованию.



### Эксперты-аналитики в области ИБ (2 человека)

Сведения по множествам угроз безопасности; объектам оценки и средствам защиты информации на предприятии поступают к экспертам-аналитикам в области ИБ с целью их анализа, корректировки, построения модели угрозы и средства защиты-объекты защиты и анализу полученной модели.

Задачи экспертов-аналитиков в области ИБ в данной деловой игре.

1. Изучить инструкцию пользователя по работе с программным обеспечением для построения модели с полным перекрытием множества угроз и подготовить программу к использованию.

2. Проанализировав сведения, внесенные в базу данных специалистами ЗИ, скорректировать данные (после проведения совместного совещания со специалистами ИТ и ЗИ).

3. Построить модель с полным перекрытием множества угроз ИБ (описание работы с программным обеспечением)

4. Проанализировать полученную модель и сделать выводы по повышению эффективности системы ИБ в организации.

5. Собрать итоговое совещание со специалистами ИТ и ЗИ, где огласить выводы и обсудить дальнейшие мероприятия по повышению эффективности системы защиты информации в рассматриваемой организации.

Подведение итогов, подробный анализ деловой игры:

1. общая оценка игры, подробный анализ реализации целей и задач, удачные и слабые стороны, их причины (проводится преподавателем);

2. самооценка участниками исполнения полученных заданий, степень личной удовлетворенности (оценки сотрудникам службы ИТ и ЗИ выставляют руководители этих служб, назначенные перед началом игры; оценка деятельности экспертов по ИБ проводится преподавателем);

3. характеристика профессиональных знаний и умений, выявленных в процессе игры (проводится преподавателем);

Критерием оценок может служить количество и содержательность выдвинутых идей (предложений), степень самостоятельности суждений, их практическая значимость. Оценивание осуществляется по десяти бальной шкале.

### **Вопросы к экзамену: «Организационно-правовое обеспечение информационной безопасности»**

1. Администрирование АИС: функции администратора, функции службы безопасности.
2. Какие механизмы безопасности используются для обеспечения "неотказуемости" системы?
3. Что понимается под администрированием средств безопасности?
4. Какие виды избыточности могут использоваться в вычислительных сетях?
5. В чем заключаются преимущества сети с выделенными каналами?
6. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
7. Виды криптосистем.
8. Задачи, решаемые методами криптографии.
9. Норма права и система права
10. Понятие, предмет и объект гражданского права
11. Принципы гражданского права
12. Источники гражданского права
13. Объекты гражданского права
14. Субъекты гражданского права

15. Структура информационной сферы, характеристика ее элементов.
16. Информация как объект правоотношений, категории информации.
17. Система правовой защиты информации.
18. Понятие и виды защищаемой информации.
19. Особенности государственной тайны как защищаемой информации.
20. Система защиты государственной тайны.
21. Засекречивание информации, отнесенной к государственной тайне.
22. Защита сведений отнесенных к государственной тайне.
23. Понятие информации конфиденциального характера.
24. Основные виды конфиденциальной информации, в соответствии с
25. требованиями российской нормативно-правовой базы.
26. Правовой режим конфиденциальной информации.
27. Основные требования, предъявляемые к организации защиты конфиденциальной информации. История криптографии. Основные этапы становления науки криптографии.
28. Методы криптографических преобразований.
29. Шифрование перестановкой.
30. Шифрование методом гаммирования и аналитического преобразования.
31. Многократное шифрование.
32. Композиция блочных шифров.
33. Совершенные шифры. Пример совершенного шифра.
34. Энтропийные характеристики шифров.
35. Идеальные шифры.
36. Стратегия национальной безопасности Российской Федерации: особенности, цели, составляющие национальных интересов России в информационной сфере.
37. Доктрина информационной безопасности Российской Федерации: назначение документа, источники угроз информационной безопасности Российской Федерации, общие методы обеспечения информационной безопасности РФ.
38. Нормативно-правовое регулирование защиты информации: направления защиты
39. Виды конфиденциальной информации: коммерческая тайна, персональные данные
40. Виды конфиденциальной информации: государственная служебная тайна, процессуальная тайна, авторское, патентное право.
41. Организационно-распорядительная защита информации: цели защиты, принципы построения защиты
42. Подготовка программы проведения конфиденциальных переговоров.
43. Порядок проведения конфиденциальных переговоров.
44. Требования режима защиты информации при приеме в организации
45. посетителей. Порядок доступа посетителей и командированных лиц к конфиденциальной информации. Порядок пребывания посетителей на территории и в помещениях организации.
46. Требования к программе приема иностранных представителей.
47. Требования к помещениям, в которых проводится прием иностранных представителей.
48. Обеспечение защиты информации при выезде за рубеж командированных лиц.
49. Основные виды и формы рекламы. Общие требования режима защиты информации в процессе рекламной деятельности.
50. Основные методы защиты информации в рекламной деятельности.
51. Понятие «публикация в открытой печати». Общие требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.
52. Особенности защиты информации при опубликовании материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.

53. Виды пропускных документов.
54. Порядок организации работы бюро пропусков.
55. Контрольно-пропускные пункты, их оборудование и организация работы.
56. Понятие «внутриобъектовый режим» и его общие требования.
57. Противопожарный режим и его обеспечение.
58. Подбор и расстановка кадров.
59. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала.
60. Основные формы обучения и методы контроля знаний.
61. Мотивация персонала к выполнению требований по защите информации.
62. Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика.
63. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.
64. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
65. Организационные меры по защите информации при увольнении сотрудника.
66. Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров.
67. Основные этапы проведения конфиденциальных переговоров.
68. Подготовка помещения для проведения конфиденциальных переговоров

#### Рекомендуемая литература

1. Деловые коммуникации в государственном и муниципальном управлении : учебное пособие для вузов / А. С. Никитина, Н. Г. Чевтаева, С. А. Ваторопин, А. С. Ваторопин. — Москва : Издательство Юрайт, 2021. — 171 с. — (Высшее образование). — ISBN 978-5-534-13964-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/467374>
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2021. — 325 с.
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забаурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование).
4. Нетёсова, О. Ю. Информационные технологии в экономике : учебное пособие для среднего профессионального образования / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 178 с. — (Профессиональное образование).
5. 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. Александр, Шилов und Владимир Мищенко Информационная безопасность финансового учреждения / Александр Шилов und Владимир Мищенко. - М.: LAP Lambert Academic Publishing, **2021**. - 164 с.
2. Артемов, А. Информационная безопасность. Курс лекций / А. Артемов. - Москва: РГГУ, **2018**. - **788** с.
3. Астахова, Л. Герменевтика в информационной безопасности / Л. Астахова. - М.: LAP Lambert Academic Publishing, **2020**. - 296 с.
4. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: моногр. . - Москва: **Мир**, **2020**. - 552 с.
5. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. Гриф УМО МО РФ / Афанасьев Алексей Алексеевич. - М.: Горячая линия - Телеком, **2020**. - **438** с.
6. Бабаш, А. В. Информационная безопасность (+ CD-ROM) / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, **2021**. - 136 с.
7. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
8. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.
9. Рассолов, И.М. Информационное право : учебник и практикум для акад. бакалавриата / И.М. Рассолов. - 4-е изд., перераб. и доп. - М. : Юрайт, 2017. - 3346 с.

### *Электронные ресурсы*

1. Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ / Дагестанский государственный университет. – Махачкала, 2010. – Режим доступа: <http://elib.dgu.ru>, свободный
2. Moodle [Электронный ресурс]: система виртуального обучения: [база данных] / Даг. Гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. –URL: <http://moodle.dgu.ru/>
3. Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ / Дагестанский гос. ун-т. – Махачкала, 2010 – режим доступа: <http://elib.dgu.ru>, свободный
4. Большой юридический справочник - [http://www.blblaw.ru/kodeksy\\_rf.html](http://www.blblaw.ru/kodeksy_rf.html)
5. Беззубцев О.А., Мартынов В.Н., Мартынов В.М. Некоторые вопросы правового обеспечения использования ЭЦП // <http://www.cioworld.ru/offline/2002/6/21492/>
6. Все о праве. Компас в мире юриспруденции – <http://www.allpravo.ru/library/>
7. Журнал «Вопросы правоведения» – <http://coop.chuvashia.ru>
8. Закон и правопорядок - <http://zakon.rin.ru>
9. Классика российского права – <http://civil.consultant.ru>
10. Кузнецов П.У. Правовая информатика. Теория. Общая часть: учебное пособие - <http://www.telecomlaw.ru/studyguides>
11. Образовательные ресурсы Интернета – юриспруденция <http://www.alleng.ru/edu/jurispr3.htm>
12. Сибирский, В. К. Правовая информатика: учебный курс (УМК). – Московский институт экономика, менеджмента и права, Центр дистанционных образовательных технологий МИЭМП - <http://www.ecollege.ru/xbooks/xbook093>