ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ ИМПЕРАТОРА ПЕТРА I»

Гуманитарно-правовой факультет

Кафедра теории и истории государства и права

«УТВЕРЖДАЮ»
Зав. кафедрой

Махина С.Н.
«31» августа 2017 г.

Фонд оценочных средств

Б1.В.ДВ.07.01 по дисциплине «Правовые основы информационной безопасности»
направлению 40.03.01 - Юриспруденция
профиль подготовки бакалавра
Государственно-правовой
квалификация (степень) выпускника – бакалавр

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 009DC7B5B98BCBFB48AE0288B7F4173114
Владелец: Агибалов Александр Владимирович
Действителен: с 09.02.2023 до 04.05.2024

1. Перечень компетенций с указанием этапов их формирования в процессе освоения учебной дисциплины «Правовые основы информационной безопасности»

Индекс	Формулировка	Разделы дисциплины		
		1	2	3
ОПК-1	способность соблюдать законодательство Российской Федерации, в том числе Конституцию Российской Федерации, федеральные конституционные законы и федеральные законы, а также общепризнанные принципы, нормы международного права и международные договоры Российской Федерации	+	+	+
ПК-3	способность обеспечивать соблюдение законодательства Российской Федерации субъектами права	+	+	+
ПК-6	способность юридически правильно квалифицировать факты и обстоятельства	+	+	+
ПК-10	способность выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения	+	+	+
ПК-11	способность осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению	+	+	+

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

2.1 Шкала академических оценок освоения дисциплины

Виды оценок	Оценки	
Академическая оценка по 2-х балльной шкале (зачет)	не зачтено	зачтено

2.2 Текущий контроль

Код	Планируемые результаты	Раздел дисциплины	Содержание требования в разрезе разделов дисциплины	Технология формирования	Форма оценочного средства (контроля)	№Задания		
						Пороговый уровень (удовл.)	Повышенный уровень (хорошо)	Высокий уровень (отлично)
ОПК-1	знать: основы российского законодательства в области правового обеспечения информационной безопасности; международные правовые акты по информационной безопасности и пределы их реализации на территории РФ; соотношение международного и российского законодательства в области обеспечения информационной безопасности РФ; уметь: применять нормы	1-3	Информационная безопасность как определяющий компонент национальной безопасности РФ. Место информационной безопасности в системе национальной безопасности РФ. Понятие, структура и содержание информационной безопасности.	Лекции, практические занятия, самостоятельная работа	Устный опрос, тестирование, доклад, решение задач	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.

	российского и международного права при обеспечении информационной безопасности; выявлять и анализировать проблемы информационной безопасности, предлагать способы преодоления выявленных проблем; иметь навыки и/или опыт деятельности: соблюдения законодательства РФ, а также общепризнанных принципов, норм международного права и международных договоры Российской Федерации в области оборота информации, подлежащей правовой защите;							
ПК-3	знать: понятийный и категориальный аппарат информационного права, основные правовые теоретические конструкции, систему нормативных правовых актов, регулирующих сферу обеспечения информационной безопасности; уметь: работать с нормативно-правовым	1-3	Законодательство в области обеспечения информационной безопасности. Классификация структура нормативных правовых актов в сфере обеспечения информационной безопасности.	Лекции, практические занятия, самостоятельная работа	Устный опрос, тестирование, доклад, решение задач	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.

	материалом, использовать и извлекать всю необходимую для решения проблемы информацию в условиях обеспечения соблюдения законодательства Российской Федерации субъектами права; иметь навыки и/или опыт деятельности: обеспечения соблюдения законодательства Российской Федерации субъектами права в области информационной безопасности.							

ПК-6	знать: формы и виды информации, подлежащей правовой охране; способы обеспечения информационной безопасности и особенности их реализации; основные виды правонарушений в сфере информационной безопасности уметь: устанавливать параметры правового регулирования соответствующего вида информации; определять особенности правового регулирования безопасного оборота информации на территории РФ и в международном пространстве; правильно квалифицировать неправомерные действия в сфере информационной безопасности иметь навыки и/или опыт деятельности: юридически правильно квалифицировать факты и обстоятельства в сфере информационной безопасности	1-3	Государственная система обеспечения информационной безопасности правового регулирования в области информационной безопасности (понятие, содержание, состав, структура, задачи).	Лекции, практические занятия, самостоятельная работа	Устный опрос, тестирование, доклад, решение задач	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.

ПК-10	знать: классификацию компьютерных преступлений и иных противоправных действий в сфере обеспечения информационной безопасности; уметь: анализировать, толковать и правильно применять правовые нормы, регулирующие вопросы выявления, пресечения, раскрытия и расследования преступлений и иные правонарушения в сфере информационной безопасности; иметь навыки и/или опыт деятельности: работы с нормативными правовыми актами, регламентирующими вопросы выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений в области информационной безопасности.	1-3	Правовая основа обеспечения защиты персональных данных. Основные положения по защите служебной тайны.	Лекции, практические занятия, самостоятельная работа	Устный опрос, тестирование, доклад, решение задач	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.

ПК-11	**знать:** современные представления о сущности информационных процессов и их безопасности, источниках информационного права, правоотношений; совокупность правовых норм в области защиты правовой информации **уметь:** разрабатывать и осуществлять мероприятия, направленные на минимизацию рисков, связанных с незнанием или неправильным применением важнейших правовых предписаний в области информационной безопасности **иметь навыки и/или опыт деятельности:** в сфере правового анализа институтов обеспечения информационной безопасности с целью предупреждения правонарушений, выявления и устранения причин и условий, способствующие их совершению	1-3	Правовая основа обеспечения защиты персональных данных. Основные положения по защите служебной тайны.	Лекции, практические занятия, самостоятельная работа	Устный опрос, тестирование, доклад, решение задач	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.	Тесты из задания п. 3.3. А, вопросы из задания п. 3.4, доклады из задания 3.5, практические задачи из п. 3.6.

2.3. Промежуточная аттестация

Код	Планируемые результаты	Технология формирования	Форма оценочного средства (контроля)	№Задания Пороговый уровень (удовл.)
ОПК-1	**знать:** основы российского законодательства в области правового обеспечения информационной безопасности; международные правовые акты по информационной безопасности и пределы их реализации на территории РФ; соотношение международного и российского законодательства в области обеспечения информационной безопасности РФ; **уметь:** применять нормы российского и международного права при обеспечении информационной безопасности; выявлять и анализировать проблемы информационной безопасности, предлагать способы преодоления выявленных проблем; **иметь навыки и/или опыт деятельности:** соблюдения законодательства РФ, а также общепризнанных принципов, норм международного права и международных договоры Российской Федерации в области оборота информации, подлежащей правовой защите;	Лекции, практические занятия, самостоятельная работа	Зачет	Вопросы из задания 3.1. Б, тесты из задания 3.3 практические задачи 3.6
ПК-3	**знать**: понятийный и категориальный аппарат информационного права, основные правовые теоретические конструкции, систему нормативных правовых актов, регулирующих сферу обеспечения информационной безопасности; **уметь:** работать с нормативно-правовым материалом, использовать и извлекать всю необходимую для решения проблемы информацию в условиях обеспечения соблюдения законодательства Российской Федерации субъектами права; **иметь навыки и/или опыт деятельности:** обеспечения соблюдения законодательства Российской Федерации субъектами права в области информационной безопасности.	Лекции, практические занятия, самостоятельная работа	Зачет	Вопросы из задания 3.1. Б, тесты из задания 3.3 практические задачи 3.6

ПК-6	**знать:** формы и виды информации, подлежащей правовой охране; способы обеспечения информационной безопасности и особенности их реализации; основные виды правонарушений в сфере информационной безопасности **уметь:** устанавливать параметры правового регулирования соответствующего вида информации; определять особенности правового регулирования безопасного оборота информации на территории РФ и в международном пространстве; правильно квалифицировать неправомерные действия в сфере информационной безопасности **иметь навыки и/или опыт деятельности:** юридически правильно квалифицировать факты и обстоятельства в сфере информационной безопасности	Лекции, практические занятия, самостоятельная работа	Зачет	Вопросы из задания 3.1. Б, тесты из задания 3.3 практические задачи 3.6
ПК-10	**знать:** классификацию компьютерных преступлений и иных противоправных действий в сфере обеспечения информационной безопасности; **уметь**: анализировать, толковать и правильно применять правовые нормы, регулирующие вопросы выявления, пресечения, раскрытия и расследования преступлений и иные правонарушения в сфере информационной безопасности; **иметь навыки и/или опыт деятельности:** работы с нормативными правовыми актами, регламентирующими вопросы выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений в области информационной безопасности.	Лекции, практические занятия, самостоятельная работа	Зачет	Вопросы из задания 3.1. Б, тесты из задания 3.3 практические задачи 3.6

ПК-11	**знать:** современные представления о сущности информационных процессов и их безопасности, источниках информационного права, правоотношений; совокупность правовых норм в области защиты правовой информации **уметь:** разрабатывать и осуществлять мероприятия, направленные на минимизацию рисков, связанных с незнанием или неправильным применением важнейших правовых предписаний в области информационной безопасности **иметь навыки и/или опыт деятельности:** в сфере правового анализа институтов обеспечения информационной безопасности с целью предупреждения правонарушений, выявления и устранения причин и условий, способствующие их совершению	Лекции, практические занятия, самостоятельная работа	Зачет	Вопросы из задания 3.1. Б, тесты из задания 3.3 практические задачи 3.6

2.4 Критерии постановки зачета

«Зачтено» по дисциплине «Региональное законодательство» выставляется по итогам проведенного текущего контроля и при выполнении заданий всех практических и лекционных занятий, рефератов и самостоятельной работы студентов. Одним из факторов при выставлении зачета является успешное выполнение итогового теста, отражающего уровень и глубину знаний студента по изучаемому курсу.

«Не зачтено» по дисциплине «Региональное законодательство» выставляется, если студент не выполняет задания практических и лекционных занятий, а также текущего контроля и самостоятельной работы. Одним из факторов при выставлении оценки «не зачтено» является безуспешное выполнение итогового теста, отражающего уровень и глубину знаний студента по изучаемому курсу.

2.5. Критерии оценки экзамена – не предусмотрены

2.6 Критерии оценки устного опроса

Оценка	Критерии
«отлично»	выставляется обучающемуся, если он четко выражает свою точу зрения по рассматриваемым вопросам, приводя соответствующие примеры
«хорошо»	выставляется обучающемуся, если он допускает отдельные погрешности в ответе
«удовлетворительно»	выставляется обучающемуся, если он обнаруживает пробелы в знаниях основного учебно-программного материала
«неудовлетворительно»	выставляется обучающемуся, если он обнаруживает существенные пробелы в знаниях основных положений учебной дисциплины, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины

2.7 Критерии оценки тестов

Ступени уровней освоения компетенций	Отличительные признаки	Показатель оценки сформированной компетенции
Пороговый	Обучающийся воспроизводит термины, основные понятия, способен узнавать языковые явления.	Не менее 55 % баллов за задания теста.
Повышенный	Обучающийся выявляет взаимосвязи, классифицирует, упорядочивает, интерпретирует, применяет на практике пройденный материал.	Не менее 75 % баллов за задания теста.
Высокий	Обучающийся анализирует, оценивает, прогнозирует, конструирует.	Не менее 90 % баллов за задания теста.
Компетенция не сформирована		Менее 55 % баллов за задания теста.

2.8 Критерии оценки докладов

Оценка	Характеристики ответа студента
Отлично	- студент глубоко и всесторонне усвоил проблему;

	- уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения
Хорошо	- студент твердо усвоил тему, грамотно и по существу излагает ее, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью; - аргументирует научные положения; - делает выводы и обобщения
Удовлетворительно	тема раскрыта недостаточно четко и полно, то есть студент освоил проблему, по существу излагает ее, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении психологических знаний; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений
Неудовлетворительно	- студент не усвоил значительной части проблемы; - допускает существенные ошибки и неточности при рассмотрении ее; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений

2.9. Критерии оценки решения типовых задач

Оценка	Характеристика решения задачи
не зачтено	Задача понята правильно, в логическом рассуждении нет существенных ошибок; однако есть существенные неточности при установлении параметров и содержания правового регулирования, выборе соответствующих правовых норм и (или) нормативных правовых актов; задача решена не полностью или в чрезмерно общем виде
зачтено	Задача понята правильно, в логическом рассуждении нет существенных ошибок; допустимы небольшие неточности при установлении параметров и содержания правового регулирования выборе соответствующих правовых норм и (или) нормативных правовых актов. В целом, задача решена полно и конкретно, получен верный ответ.

3. Контрольные задания, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения учебной дисциплины «Правовые основы информационной безопасности в РФ»

3.1 Вопросы к зачету

1. Место информационной безопасности в системе национальной безопасности РФ.
2. Понятие, структура и содержание информационной безопасности.
3. Понятие и классификация угроз информационной безопасности.
4. Угрозы информационной безопасности личности, обществу и государству.
5. Понятие и сущность комплексной защиты информации.
6. Государственная политика РФ в сфере информационной безопасности личности, общества, государства (понятие, основные направления).
7. Законодательство в области обеспечения информационной безопасности.
8. Классификация и структура нормативных правовых актов в сфере обеспечения информационной безопасности.
9. Конституция о правах и обязанностях граждан России в сфере обеспечения информационной безопасности.
10. Международно-правовые аспекты защиты информации.
11. Информация как объект правоотношений в сфере обеспечения информационной безопасности.
12. Понятие и виды защищаемой информации.
13. Государственная тайна как особый вид защищаемой информации.
14. Правовая основа обеспечения защиты государственной тайны.
15. Организация защиты государственной тайны.
16. Правовая основа защиты налоговой тайны.
17. Правовая основа защиты коммерческой тайны.
18. Правовая основа защиты банковской тайны.
19. Правовая основа защиты служебной тайны.
20. Правовая основа защиты врачебной тайны.
21. Правовая основа обеспечения защиты персональных данных.
22. Государственная система обеспечения информационной безопасности (понятие, содержание, состав, структура, задачи).
23. Организационная основа системы информационной безопасности РФ.
24. Функции элементов организационной основы системы информационной безопасности РФ.
25. Методы и формы организации защиты конфиденциальной информации.
26. Основные понятия и положения системы государственного лицензирования.
27. Организационная структура системы государственного лицензирования.
28. Система сертификации в области защиты информации.
29. Особенности сертификации средств защиты информации.
30. Ответственность за правонарушения в сфере лицензирования и сертификации.
31. Основные положения аттестации объектов информатизации по требованиям безопасности информации.
32. Защита интеллектуальной собственности в системе правового регулирования информационной безопасности.

33. Авторское право в системе правового регулирования информационной безопасности.

34. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.

35. Защита объектов промышленной собственности на основе патентов.

36. Понятие и классификация видов компьютерных правонарушений.

37. Основы расследования преступлений в сфере компьютерной информации.

38. Юридическая ответственность за нарушение правовых норм защиты информации.

39. Понятие юридической ответственности за нарушение правовых норм в области информационной безопасности.

40. Виды юридической ответственности за нарушение правовых норм в области информационной безопасности.

41. Уголовная ответственность за нарушение правовых норм в сфере информационной безопасности.

42. Административная ответственность за нарушения правовых норм в сфере информационной безопасности.

43. Особенности юридической ответственности за нарушения норм информационной безопасности в области трудовых и гражданско-правовых отношений.

44. Способы совершения компьютерных преступлений.

45. Международное сотрудничество в области противодействия преступлениям в сфере информационной безопасности.

46. Противодействие незаконного использования специальных технических средств, предназначенных для негласного получения информации.

47. Информационная война как угроза информационной безопасности.

48. Противодействие преступлениям, связанным с изготовлением банковских карт.

3.2 Вопросы к экзамену – не предусмотрено

3.3. Тестовые задания

А. Тестовые задания для проведения текущего контроля знаний обучающихся

Раздел 1. Основные понятия в области информационной безопасности

1. Что такое защита информации?

а) Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

б) Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность.

в) Деятельность, направленная на предотвращение НСД к информации.

г) Деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию.

2. Несанкционированный доступ (НСД) к информации – это:

а) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС);

б) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств;

в) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа;

г) совокупность объекта разведки, средства разведки, среды распространения сигнала.

3. Безопасность информации – это:

а) состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;

б) состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства;

в) реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность;

г) деятельность, направленная на предотвращение НСД к информации.

4. Система защиты информации – это:

а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

б) заранее намеченный результат защиты информации;

в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

г) порядок и правила применения определенных принципов и средств защиты информации.

5. Что такое «национальная безопасность»?

а) совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер;

б) система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу;

в) состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

г) состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

6. Информационная безопасность Российской Федерации – это:

а) состояние защищенности информации, циркулирующей в обществе;

б) состояние правовой защищенности информационных ресурсов,

информационных продуктов, информационных услуг;

в) состояние защищенности информационных ресурсов, обеспечивающее их формирование, использование и развитие в интересах граждан, организаций, государства;

г) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

7. Что такое угроза безопасности информации в соответствии с Национальным стандартом РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006)?

а) потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам;

б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

в) состояние, в котором находится объект безопасности вследствие возникновения неблагоприятных факторов;

г) возможность реализации воздействия на информацию, обрабатываемую АС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

8. Правовая защита информации – это:

а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

б) защита информации с помощью ее криптографического преобразования;

в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

9. Цель защиты информации – это:

а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

б) заранее намеченный результат защиты информации;

в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

г) порядок и правила применения определенных принципов и средств защиты информации.

10. Лицензирование в области защиты информации – это:

а) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ;

б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;

в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации;

г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

11. Сертификация на соответствие требованиям по безопасности информации – это:

а) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ;

б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;

в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации;

г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

12. Объект информатизации – это:

а) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объектов информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения или объекты, предназначенные для ведения конфиденциальных переговоров;

б) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

в) помещения, оборудованные средствами специальной связи;

г) содержащаяся в базах данных информации.

13. Защищаемая информация – это:

а) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

б) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

в) информация, основанная на документах, фактах;

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

14. Состояние информации, при котором ее изменение осуществляется только преднамеренно субъектами, имеющими на него право – это:

а) конфиденциальность;

б) целостность;

в) доступность;

г) помехоустойчивость.

15. Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право – это:

а) конфиденциальность;

б) целостность*;*

в) доступность;

г) безопасность.

16. Состояние информации, при котором субъекты, имеющие право доступа, могут реализовать его беспрепятственно – это:

а) конфиденциальность;

б) целостность*;*

в) доступность;

г) безопасность.

17. Объект защиты информации – это:

а) информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации;

б) совокупность объекта разведки, средства разведки, среды распространения сигнала.

в) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

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

18. Носитель защищаемой информации – это:

а) свойство материальных объектов и явлений порождать многообразие состояний, которые посредством взаимодействий передаются другим объектам и запечатлеваются в их структуре;

б) смысловое содержание объективной информации об объектах и процессах материального мира, сформированное сознанием человека с помощью смысловых образов;

в) физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

г) документ, содержащий достигнутые результаты или свидетельства осуществленной деятельности.

Раздел 2. Правовое регулирование информационной безопасности в РФ

1. Каким нормативным правовым документом утверждена Доктрина информационной безопасности?

а) Указ Президента РФ №136 от 16.03.2015 г.

б) ФЗ от 27.07.2006 г. №152

в) Постановление Правительства РФ №1233 от 3.11.1993 г.

г) Указ Президента РФ №646 от 6.12.2016 г.

2. В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные системы не включают в себя:

а) государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

б) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

в) иные информационные системы;

г) частные информационные системы.

3. Базовым законом, регулирующим информационные отношения является:

а) ФЗ «О коммерческой тайне»;

б) Закон РФ «Об авторском праве и смежных правах»;

в) ФЗ «Об информации, информационных технологиях и защите информации»;

г) ФЗ «Об архивном деле».

4. Понятие информационной инфраструктуры Российской Федерации закреплено в:

а) Конституции РФ;

б) Федеральном законе от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

в) Доктрине информационной безопасности РФ;

г) не закреплено в нормативных правовых документах.

5. В соответствии с частью 3 статьи 29 Конституции Российской Федерации каждый имеет право свободно:

а) искать и распространять информацию любым способом;

б) искать, получать, передавать, производить и распространять информацию любым законным способом;

в) искать, получать, передавать, производить и распространять информацию любым способом;

г) получать и распространять информацию любым способом.

6. Федеральный закон от 27 июля 2006 г. «О персональных данных» не регулирует отношения, возникающие при:

а) обработке персональных данных, отнесенных к государственной тайне;

б) хранении, комплектовании, учете и использовании архивных документов;

в) обработке персональных данных, отнесенных к служебной тайне;

г) включении в Единый государственный реестр индивидуальных предпринимателей.

7. Каким нормативным правовым документом утвержден перечень сведений конфиденциального характера?

а) Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203;

б) Указом Президента Российской Федерации от 6 марта 1997 г. № 188;

в) Постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870;

г) Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

8. Служебная информация ограниченного распространения – это:

а) акт законодательства, устанавливающий правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

б) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

в) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

г) информация, основанная на документах, фактах.

9. Допуск гражданина к сведениям, составляющим государственную тайну, может быть прекращен в случае:

а) перевода и приема гражданина на работу в подразделение по защите государственной тайны, шифровальные или мобилизационные органы;

б) возвращения из длительных (свыше 6 месяцев) заграничных командировок;

в) однократного нарушения им предусмотренных трудовым договором (контрактом) обязательств, связанных с сохранением государственной тайны;

г) вступления гражданина в брак, за исключением случаев, когда оба супруга работают в одной организации и имеют допуск по второй или третьей форме.

10. В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация – это:

а) сведения (сообщения, данные) независимо от формы их представления;

б) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

в) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

г) сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации.

11. В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под персональными данными понимается:

а) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

б) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

в) зафиксированная на материальном носителе информация о личности с реквизитами,

позволяющими ее идентифицировать;

г) сведения, касающиеся личности, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности.

12. В соответствии с п. 3 ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» по категории доступа информация делится на:

а) общедоступную информацию и информацию с ограниченным доступом (информация ограниченного доступа);

б) открытую и конфиденциальную;

в) конфиденциальную и секретную;

г) служебную информацию ограниченного доступа и общедоступную.

13. Что из перечисленного является основанием для рассекречивания сведений, составляющих государственную тайну:

а) отсутствие в органах государственной власти Перечня сведений, составляющих государственную тайну;

б) принятие на себя обязательств перед государством по нераспространению сведений, составляющих государственную тайну;

в) *взятие на себя Россией обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну;*

г) отсутствие специальных помещений для хранения документов, содержащих сведения, составляющие государственную тайну.

14. Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется:

а) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно;

б) для доставки почтовых отправлений;

в) в целях профессиональной деятельности журналиста;

г) в целях профессиональной деятельности оператора.

15. Открытость информации в архивных фондах обеспечивается:

а) различными режимами доступа к информации и переходом информации из одной категории доступа в другую;

б) различными режимами доступа к информации;

в) переходом информации из одной категории доступа в другую;

г) правовым статусом архивного фонда.

16. Что такое коммерческая тайна?

а) сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

б) *режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;*

в) сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны;

г) защищаемая законом информация, доверенная или ставшая известной лицу (держателю информации) исключительно в силу исполнения им профессиональных обязанностей, не связанная с государственной или муниципальной службой.

17. В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» электронная подпись - это:

а) электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра;

б) информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

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

г) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

18. В соответствии с Федеральным законом от 27.07.2010 N 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» к инсайдерской информации не относится:

а) информация о принятых решениях об итогах торгов (тендеров);

б) информация, полученная в ходе проводимых проверок, а также информация о результатах таких проверок;

в) информация о принятых решениях в отношении лиц, определенных ФЗ № 224, о выдаче, приостановлении действия или об аннулировании (отзыве) лицензий (разрешений, аккредитаций) на осуществление определенных видов деятельности, а также иных разрешений;

г) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну).

19. Каким нормативным правовым документом регламентированы вопросы защиты интеллектуальной собственности в Российской Федерации?

а) Законом РФ от 23.09.1992 N 3526-1 «О правовой охране топологий интегральных микросхем»;

б) *Гражданским кодексом Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ;*

в) Законом РФ от 09.07.1993 № 5351-1 «Об авторском праве и смежных правах»;

г) Патентным законом Российской Федерации от 23.09.1992 № 3517-1.

20. Объектами авторского права не являются:

а) программы для электронных вычислительных машин (программы для ЭВМ);

б) литературные произведения;

в) изобретения;

г) аудиовизуальные произведения.

21. Объектами патентного права не являются:

а) программы для электронных вычислительных машин (программы для ЭВМ);

б) полезные модели;

в) промышленные образцы;

г) изобретения.

22. Какие элементы включает знак охраны авторского права:

а) латинская буква «С» в окружности, имя или наименование правообладателя, год первого опубликования произведения;

б) латинская буква «С» в окружности, имя или наименование автора, год первого опубликования произведения;

в) латинская буква «С» в окружности, псевдоним автора, год первого опубликования произведения;

г) латинская буква «С» в окружности, имя или наименование автора.

23. Несут ли ответственность лица, виновные в нарушении норм, регулирующих обработку и защиту информации?

а) несут только дисциплинарную и уголовную ответственность;

б) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном действующим законодательством;

в) несут только дисциплинарную и административную ответственность;

г) не несут.

24. Какой вид ответственности наступает в случае совершения следующих действий: незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере?

а) административная ответственность;

б) уголовная ответственность;

в) дисциплинарная ответственность;

г) гражданско-правовая ответственность.

25. Какой вид ответственности наступает в случае совершения следующих действий: ввоз, продажа, сдача в прокат или иное незаконное использование экземпляров произведений или фонограмм в целях извлечения дохода в случаях, если экземпляры произведений или фонограмм являются контрафактными в соответствии с законодательством Российской Федерации об авторском праве и смежных правах либо на экземплярах произведений или фонограмм указана ложная информация об их изготовителях, о местах их производства, а также об обладателях авторских и смежных прав, а равно иное нарушение авторских и смежных прав в целях извлечения дохода?

а) административная ответственность;

б) уголовная ответственность;

в) дисциплинарная ответственность;

г) гражданско-правовая ответственность.

26. Какой вид ответственности предусмотрен действующим законодательством в случае нарушения условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)?

а) уголовная ответственность;

б) административная ответственность;

в) дисциплинарная ответственность;

г) гражданско-правовая ответственность.

27. Какой вид ответственности предусмотрен действующим законодательством в случае использования несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну)?

а) уголовная ответственность;

б) административная ответственность;

в) дисциплинарная ответственность;

г) гражданско-правовая ответственность.

28. Общественно опасными последствиями в соответствии со ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» являются:

а) уничтожение компьютерной информации;

б) модификация либо копирование компьютерной информации;

в) блокирование компьютерной информации;

г) все вышеперечисленное.

29. Какой ущерб признается крупным в статьях главы 28 УК РФ «Преступления в сфере компьютерной информации»:

а) ущерб, сумма которого превышает пятьсот тыс. рублей;

б) ущерб, сумма которого превышает один миллион рублей;

в) ущерб, сумма которого превышает два миллиона рублей;

г) ущерб, сумма которого превышает сто тыс. рублей.

30. В каких формах выражается государственная измена в соответствии со ст. 275 УК РФ?

а) государственная измена в форме шпионажа;

б) государственная измена в форме выдачи государственной тайны;

в) государственная измена в форме оказания помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности против России;

г) все вышеперечисленное.

31. Допускается ли освобождение от уголовной ответственности лица, совершившего преступления, предусмотренные ст. ст. 275, 276?

а) нет, не допускается;

б) допускается, если оно своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации;

в) допускается, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба

интересам Российской Федерации и если в его действиях не содержится иного состава преступления;

г) допускается, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации.

32. Кто является субъектом преступления, предусмотренного ст. 276 УК РФ?

а) гражданин РФ;

б) иностранный гражданин или лицо без гражданства;

в) государственный служащий;

г) лицо, которому государственная тайна была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации.

33. В соответствии с Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне» государственная тайна – это:

а) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

б) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

в) информация, основанная на документах, фактах;

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

Раздел 3. Государственная система обеспечения информационной безопасности российской Федерации

1. На какой орган исполнительной власти РФ возлагается функция уполномоченного органа по защите прав субъектов персональных данных?

а) Федеральную службу охраны Российской Федерации (ФСО России);

б) Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

в) Федеральную службу безопасности Российской Федерации (ФСБ России);

г) Федеральную службу по техническому и экспортному контролю (ФСТЭК России).

2. Какой орган исполнительной власти РФ осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации?

а) ФСБ России;

б) МВД России;

в) ФСО России;

г) ФСТЭК России.

3. Что является организационной формой защиты информации?

а) разработка и реализация специальных законов, нормативных правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) *регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;*

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения;

г) формирование правового статуса всех субъектов в системе информационной безопасности и определение их ответственности за обеспечение информационной безопасности.

4. Что является объектом системы сертификации:

а) вид деятельности;

б) помещения;

в) средства защиты информации;

г) автоматизированные системы.

5. Какой из перечисленных видов деятельности не подлежит обязательному лицензированию?

а) деятельность, связанная с защитой государственной тайны;

б) работа со сведениями, составляющими конфиденциальную информацию;

в) разработка и производство средств защиты конфиденциальной информации;

г) деятельность по технической защите конфиденциальной информации.

6. В соответствии с Постановлением Правительства РФ от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» органами, уполномоченными на ведение лицензионной деятельности на право проведения работ, связанных с созданием средств защиты информации, являются:

а) Служба внешней разведки Российской Федерации;

б) Министерство обороны Российской Федерации;

в) Федеральная служба безопасности Российской Федерации (в пределах ее компетенции);

г) все перечисленные органы.

7. Каков срок действия лицензии в зависимости от специфики вида деятельности?

1. лицензия действует бессрочно;
2. не более 3 лет;
3. не более 4 лет;
4. *не более 5 лет.*

8. Каким нормативным правовым документом регламентированы вопросы выдачи/получения лицензии на осуществление деятельности, связанной с защитой государственной тайны?

а) Постановлением Правительства РФ от 15.04.1995 № 333;

б) Постановлением Правительства РФ от 16.04.2012 № 313;

в) Постановлением Правительства РФ от 03.03.2012 № 171;

г) Постановлением Правительства РФ от 16.04.2012 № 314.

9. Каким нормативным правовым документом регламентированы вопросы выдачи/получения лицензии на осуществление деятельности, по разработке и производству средств защиты конфиденциальной информации?

а) Постановлением Правительства РФ от 15.04.1995 № 333;

б) Постановлением Правительства РФ от 16.04.2012 № 313;

в) Постановлением Правительства РФ от 03.03.2012 № 171;

г) Постановлением Правительства РФ от 16.04.2012 № 314.

10. В соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» к полномочиям лицензирующих органов не относится:

а) осуществление лицензирования конкретных видов деятельности;

б) проведение мониторинга эффективности лицензирования, подготовка и представление ежегодных докладов о лицензировании;

в) утверждение форм заявлений о предоставлении лицензий, переоформлении лицензий, а также форм уведомлений, предписаний об устранении выявленных нарушений лицензионных требований, выписок из реестров лицензий и других используемых в процессе лицензирования документов;

г) утверждение типовой формы лицензии.

11. Что означает термин «лицензиат»?

а) юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии;

б) юридическое лицо или индивидуальный предприниматель, имеющие лицензию;

в) уполномоченные на выдачу лицензии на ведение того или иного вида деятельности федеральные органы исполнительной власти;

г) вид деятельности, подлежащий обязательному лицензированию.

12. Что не входит в перечень документов, необходимых для получения лицензии в соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ (ред. от 30.12.2015) «О лицензировании отдельных видов деятельности»?

а) копии документов, перечень которых определяется положением о лицензировании конкретного вида деятельности;

б) заявление на получение лицензии;

в) опись прилагаемых документов;

г) документ, подтверждающий уплату государственной пошлины за предоставление лицензии.

13. Что из перечисленного не является основанием для отказа в предоставлении лицензии?

а) наличие лицензии на ведение иного вида деятельности;

б) наличие в представленных соискателем лицензии заявлении о предоставлении лицензии и (или) прилагаемых к нему документах недостоверной или искаженной информации;

в) установленное в ходе проверки несоответствие соискателя лицензии лицензионным требованиям;

г) представление соискателем лицензии заявления о предоставлении лицензии и прилагаемых к этому заявлению документов, если в отношении соискателя лицензии имеется решение об аннулировании ранее выданной лицензии на такой вид деятельности.

14. Не входят в организационную структуру системы сертификации в соответствии с «Положением о сертификации средств защиты информации по

требованиям безопасности информации» (утв. Приказом Гостехкомиссии РФ от 27.10.1995 № 199):

а) органы по аттестации объектов информатизации по требованиям безопасности информации;

б) органы по сертификации средств защиты информации;

в) испытательные центры (лаборатории);

г) заявители.

15. На какой элемент организационной структуры системы сертификации возложена функция по ведению государственного реестра участников и объектов сертификации:

а) федеральный орган по сертификации средств защиты информации;

б) центральный орган системы сертификации средств защиты информации;

в) органы по сертификации средств защиты информации;

г) испытательные центры (лаборатории).

16. На какой элемент организационной структуры системы сертификации возложена функция по проведению экспертизы технической, эксплуатационной документации на средства защиты информации и материалов сертификационных испытаний:

а) федеральный орган по сертификации средств защиты информации;

б) центральный орган системы сертификации средств защиты информации;

в) органы по сертификации средств защиты информации;

г) испытательные центры (лаборатории).

17. На какой элемент организационной структуры системы сертификации возложена функция по разработке программы и методики сертификационных испытаний, осуществлению сертификационных испытаний средств защиты информации?

а) федеральный орган по сертификации средств защиты информации;

б) центральный орган системы сертификации средств защиты информации;

в) органы по сертификации средств защиты информации;

г) испытательные центры (лаборатории).

18. Целью создания системы сертификации является:

а) *реализация требований государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам;*

б) предотвращение ущерба безопасности государства, возможность нанесения которого связана с осуществлением юридическими лицами и индивидуальными предпринимателями отдельных видов деятельности;

в) проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

г) подтверждение соответствия объекта информатизации требованиям по безопасности информации.

19. Целью создания системы лицензирования является:

а) реализация требований государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам;

б) предотвращение ущерба безопасности государства, возможность нанесения которого связана с осуществлением юридическими лицами и индивидуальными предпринимателями отдельных видов деятельности;

в) проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

г) подтверждение соответствия объекта информатизации требованиям по безопасности информации.

Б. Тестовые задания для проведения промежуточной аттестации обучающихся

Вариант 1

1. Что такое защита информации?

а) Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

б) Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность.

в) Деятельность, направленная на предотвращение НСД к информации.

г) Деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию.

2. Безопасность информации – это:

а) состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;

б) состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства;

в) реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность;

г) деятельность, направленная на предотвращение НСД к информации.

3. Что такое «национальная безопасность»?

а) совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер;

б) система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу;

в) состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

г) состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

4. Что такое угроза безопасности информации в соответствии с Национальным стандартом РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006)?

а) потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам;

б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

в) состояние, в котором находится объект безопасности вследствие возникновения неблагоприятных факторов;

г) возможность реализации воздействия на информацию, обрабатываемую АС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

5. Сертификация на соответствие требованиям по безопасности информации – это:

а) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ;

б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;

в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации;

г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

6. Защищаемая информация – это:

а) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

б) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

в) информация, основанная на документах, фактах;

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

7. Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право – это:

а) конфиденциальность;

б) целостность*;*

в) доступность;

г) безопасность.

8. Объект защиты информации – это:

а) информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации;

б) совокупность объекта разведки, средства разведки, среды распространения сигнала.

в) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

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

9. Каким нормативным правовым документом утверждена Доктрина информационной безопасности?

а) Указ Президента РФ №136 от 16.03.2015 г.

б) ФЗ от 27.07.2006 г. №152

в) Постановление Правительства РФ №1233 от 3.11.1993 г.

г) Указ Президента РФ №646 от 6.12.2016 г.

10. Базовым законом, регулирующим информационные отношения является:

а) ФЗ «О коммерческой тайне»;

б) Закон РФ «Об авторском праве и смежных правах»;

в) ФЗ «Об информации, информационных технологиях и защите информации»;

г) ФЗ «Об архивном деле».

11. В соответствии с частью 3 статьи 29 Конституции Российской Федерации каждый имеет право свободно:

а) искать и распространять информацию любым способом;

б) искать, получать, передавать, производить и распространять информацию любым законным способом;

в) искать, получать, передавать, производить и распространять информацию любым способом;

г) получать и распространять информацию любым способом.

12. Каким нормативным правовым документом утвержден перечень сведений конфиденциального характера?

а) Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203;

б) Указом Президента Российской Федерации от 6 марта 1997 г. № 188;

в) Постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870;

г) Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

13. Допуск гражданина к сведениям, составляющим государственную тайну, может быть прекращен в случае:

а) перевода и приема гражданина на работу в подразделение по защите государственной тайны, шифровальные или мобилизационные органы;

б) возвращения из длительных (свыше 6 месяцев) заграничных командировок;

в) однократного нарушения им предусмотренных трудовым договором (контрактом) обязательств, связанных с сохранением государственной тайны;

г) вступления гражданина в брак, за исключением случаев, когда оба супруга работают в одной организации и имеют допуск по второй или третьей форме.

14. В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под персональными данными понимается:

а) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

б) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

в) зафиксированная на материальном носителе информация о личности с реквизитами, позволяющими ее идентифицировать;

г) сведения, касающиеся личности, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности.

15. Что из перечисленного является основанием для рассекречивания сведений, составляющих государственную тайну:

а) отсутствие в органах государственной власти Перечня сведений, составляющих государственную тайну;

б) принятие на себя обязательств перед государством по нераспространению сведений, составляющих государственную тайну;

в) *взятие на себя Россией обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну;*

г) отсутствие специальных помещений для хранения документов, содержащих сведения, составляющие государственную тайну.

16. В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» электронная подпись - это:

а) электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра;

б) информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

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

г) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

17. Каким нормативным правовым документом регламентированы вопросы защиты интеллектуальной собственности в Российской Федерации?

а) Законом РФ от 23.09.1992 N 3526-1 «О правовой охране топологий интегральных микросхем»;

б) *Гражданским кодексом Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ;*

в) Законом РФ от 09.07.1993 № 5351-1 «Об авторском праве и смежных правах»;

г) Патентным законом Российской Федерации от 23.09.1992 № 3517-1.

18. Несут ли ответственность лица, виновные в нарушении норм, регулирующих обработку и защиту информации?

а) несут только дисциплинарную и уголовную ответственность;

б) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном действующим законодательством;

в) несут только дисциплинарную и административную ответственность;

г) не несут.

19. Какой вид ответственности предусмотрен действующим законодательством в случае использования несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну)?

а) уголовная ответственность;

б) административная ответственность;

в) дисциплинарная ответственность;

г) гражданско-правовая ответственность.

20. В соответствии с Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне» государственная тайна – это:

а) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

б) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

в) информация, основанная на документах, фактах;

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

21. На какой орган исполнительной власти РФ возлагается функция уполномоченного органа по защите прав субъектов персональных данных?

а) Федеральную службу охраны Российской Федерации (ФСО России);

б) Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

в) Федеральную службу безопасности Российской Федерации (ФСБ России);

г) Федеральную службу по техническому и экспортному контролю (ФСТЭК России).

22. Какой из перечисленных видов деятельности не подлежит обязательному лицензированию?

а) деятельность, связанная с защитой государственной тайны;

б) работа со сведениями, составляющими конфиденциальную информацию;

в) разработка и производство средств защиты конфиденциальной информации;

г) деятельность по технической защите конфиденциальной информации.

23. Что означает термин «лицензиат»?

а) юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии;

б) юридическое лицо или индивидуальный предприниматель, имеющие лицензию;

в) уполномоченные на выдачу лицензии на ведение того или иного вида деятельности федеральные органы исполнительной власти;

г) вид деятельности, подлежащий обязательному лицензированию.

24. Что из перечисленного не является основанием для отказа в предоставлении лицензии?

а) наличие лицензии на ведение иного вида деятельности;

б) наличие в представленных соискателем лицензии заявлении о предоставлении лицензии и (или) прилагаемых к нему документах недостоверной или искаженной информации;

в) установленное в ходе проверки несоответствие соискателя лицензии лицензионным требованиям;

г) представление соискателем лицензии заявления о предоставлении лицензии и прилагаемых к этому заявлению документов, если в отношении соискателя лицензии имеется решение об аннулировании ранее выданной лицензии на такой вид деятельности.

25. Целью создания системы лицензирования является:

а) реализация требований государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам;

б) предотвращение ущерба безопасности государства, возможность нанесения которого связана с осуществлением юридическими лицами и индивидуальными предпринимателями отдельных видов деятельности;

в) проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

г) подтверждение соответствия объекта информатизации требованиям по безопасности информации.

Вариант 2.

1. Система защиты информации – это:

а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

б) заранее намеченный результат защиты информации;

в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

г) порядок и правила применения определенных принципов и средств защиты информации.

2. Информационная безопасность Российской Федерации – это:

а) состояние защищенности информации, циркулирующей в обществе;

б) состояние правовой защищенности информационных ресурсов, информационных продуктов, информационных услуг;

в) состояние защищенности информационных ресурсов, обеспечивающее их формирование, использование и развитие в интересах граждан, организаций, государства;

г) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

3. Правовая защита информации – это:

а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

б) защита информации с помощью ее криптографического преобразования;

в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

4. Лицензирование в области защиты информации – это:

а) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ;

б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;

в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации;

г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

5. Состояние информации, при котором ее изменение осуществляется только преднамеренно субъектами, имеющими на него право – это:

а) конфиденциальность;

б) целостность;

в) доступность;

г) помехоустойчивость.

6. Носитель защищаемой информации – это:

а) свойство материальных объектов и явлений порождать многообразие состояний, которые посредством взаимодействий передаются другим объектам и запечатлеваются в их структуре;

б) смысловое содержание объективной информации об объектах и процессах материального мира, сформированное сознанием человека с помощью смысловых образов;

в) физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

г) документ, содержащий достигнутые результаты или свидетельства осуществленной деятельности.

7. Понятие информационной инфраструктуры Российской Федерации

закреплено в:

а) Конституции РФ;

б) Федеральном законе от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

в) Доктрине информационной безопасности РФ;

г) не закреплено в нормативных правовых документах.

8. Федеральный закон от 27 июля 2006 г. «О персональных данных» не регулирует отношения, возникающие при:

а) обработке персональных данных, отнесенных к государственной тайне;

б) хранении, комплектовании, учете и использовании архивных документов;

в) обработке персональных данных, отнесенных к служебной тайне;

г) включении в Единый государственный реестр индивидуальных предпринимателей.

9. Служебная информация ограниченного распространения – это:

а) акт законодательства, устанавливающий правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

б) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

в) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

г) информация, основанная на документах, фактах.

10. В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация – это:

а) сведения (сообщения, данные) независимо от формы их представления;

б) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

в) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

г) сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации.

11. В соответствии с п. 3 ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» по категории доступа информация делится на:

а) общедоступную информацию и информацию с ограниченным доступом (информация ограниченного доступа);

б) открытую и конфиденциальную;

в) конфиденциальную и секретную;

г) служебную информацию ограниченного доступа и общедоступную.

12. Что такое коммерческая тайна?

а) сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

б) *режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;*

в) сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны;

г) защищаемая законом информация, доверенная или ставшая известной лицу (держателю информации) исключительно в силу исполнения им профессиональных обязанностей, не связанная с государственной или муниципальной службой.

13. В соответствии с Федеральным законом от 27.07.2010 N 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» к инсайдерской информации не относится:

а) информация о принятых решениях об итогах торгов (тендеров);

б) информация, полученная в ходе проводимых проверок, а также информация о результатах таких проверок;

в) информация о принятых решениях в отношении лиц, определенных ФЗ № 224, о выдаче, приостановлении действия или об аннулировании (отзыве) лицензий (разрешений, аккредитаций) на осуществление определенных видов деятельности, а также иных разрешений;

г) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну).

14. Объектами авторского права не являются:

а) программы для электронных вычислительных машин (программы для ЭВМ);

б) литературные произведения;

в) изобретения;

г) аудиовизуальные произведения.

15. Какие элементы включает знак охраны авторского права:

а) латинская буква «С» в окружности, имя или наименование правообладателя, год первого опубликования произведения;

б) латинская буква «С» в окружности, имя или наименование автора, год первого опубликования произведения;

в) латинская буква «С» в окружности, псевдоним автора, год первого опубликования произведения;

г) латинская буква «С» в окружности, имя или наименование автора.

16. Какой вид ответственности предусмотрен действующим законодательством в случае нарушения условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)?

а) уголовная ответственность;

б) административная ответственность;

в) дисциплинарная ответственность;

г) гражданско-правовая ответственность.

17. Общественно опасными последствиями в соответствии со ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» являются:

а) уничтожение компьютерной информации;

б) модификация либо копирование компьютерной информации;

в) блокирование компьютерной информации;

г) все вышеперечисленное.

18. В каких формах выражается государственная измена в соответствии со ст. 275 УК РФ?

а) государственная измена в форме шпионажа;

б) государственная измена в форме выдачи государственной тайны;

в) государственная измена в форме оказания помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности против России;

г) все вышеперечисленное.

19. Какой орган исполнительной власти РФ осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации?

а) ФСБ России;

б) МВД России;

в) ФСО России;

г) ФСТЭК России.

20. Что является объектом системы сертификации:

а) вид деятельности;

б) помещения;

в) средства защиты информации;

г) автоматизированные системы.

21. В соответствии с Постановлением Правительства РФ от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» органами, уполномоченными на ведение лицензионной деятельности на право проведения работ, связанных с созданием средств защиты информации, являются:

а) Служба внешней разведки Российской Федерации;

б) Министерство обороны Российской Федерации;

в) Федеральная служба безопасности Российской Федерации (в пределах ее компетенции);

г) все перечисленные органы.

22. Каким нормативным правовым документом регламентированы вопросы выдачи/получения лицензии на осуществление деятельности, связанной с защитой государственной тайны?

а) Постановлением Правительства РФ от 15.04.1995 № 333;

б) Постановлением Правительства РФ от 16.04.2012 № 313;

в) Постановлением Правительства РФ от 03.03.2012 № 171;

г) Постановлением Правительства РФ от 16.04.2012 № 314.

23. В соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» к полномочиям лицензирующих органов не относится:

а) осуществление лицензирования конкретных видов деятельности;

б) проведение мониторинга эффективности лицензирования, подготовка и представление ежегодных докладов о лицензировании;

в) утверждение форм заявлений о предоставлении лицензий, переоформлении лицензий, а также форм уведомлений, предписаний об устранении выявленных нарушений лицензионных требований, выписок из реестров лицензий и других используемых в процессе лицензирования документов;

г) утверждение типовой формы лицензии.

24. Что не входит в перечень документов, необходимых для получения лицензии в соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ (ред. от 30.12.2015) «О лицензировании отдельных видов деятельности»?

а) копии документов, перечень которых определяется положением о лицензировании конкретного вида деятельности;

б) заявление на получение лицензии;

в) опись прилагаемых документов;

г) документ, подтверждающий уплату государственной пошлины за предоставление лицензии.

25. Не входят в организационную структуру системы сертификации в соответствии с «Положением о сертификации средств защиты информации по требованиям безопасности информации» (утв. Приказом Гостехкомиссии РФ от 27.10.1995 № 199):

а) органы по аттестации объектов информатизации по требованиям безопасности информации;

б) органы по сертификации средств защиты информации;

в) испытательные центры (лаборатории);

г) заявители.

3.4 Примерный перечень вопросов для устного опроса

1. Что такое информационная безопасность?
2. Что относится к основным принципам обеспечения безопасности?
3. Раскройте понятие «угроза национальной безопасности».
4. Раскройте понятие «система обеспечения национальной безопасности».
5. Что относится к национальным интересам в информационной сфере?
6. Что составляет организационную основу системы обеспечения информационной безопасности?
7. На каких принципах основывается деятельность государственных органов по обеспечению информационной безопасности?

8. Что такое правовое обеспечение информационной безопасности?
9. Каково содержание правового обеспечения информационной безопасности?
10. Раскройте содержание уровней системы правовой защиты информации.
11. Перечислите цели правовой защиты информации.
12. Дайте определение информационным правоотношениям.
13. Раскройте содержание информационного законодательства как самостоятельной отрасли права.
14. Что понимается под законодательством в области обеспечения информационной безопасности?
15. Что такое нормативный правовой акт?
16. Приведите классификацию нормативных правовых актов по юридической силе.
17. Перечислите основные международные правовые акты в области информационной безопасности.
18. Перечислите основные нормативные правовые акты федерального уровня в области информационной безопасности.
19. Перечислите основные концептуальные документы в области информационной безопасности.
20. Перечислите основные подзаконные нормативные документы в области информационной безопасности.
21. Каково содержание Конституции Российской Федерации о правах и обязанностях граждан России в сфере обеспечения информационной безопасности?
22. Что понимается под информационной сферой как сферой правового регулирования?
23. Приведите известные Вам понятия «информация».
24. Что означает термин «целостность информации»?
25. Что означает термин «доступность информации»?
26. Что означает термин «конфиденциальность информации»?
27. Что такое защищаемая информация и каковы ее отличительные признаки?
28. Перечислите известные Вам критерии классификации защищаемой информации.
29. К какой информации не может быть ограничен доступ?
30. Какие сведения относятся к информации с ограниченным доступом?
31. Что понимается под термином «государственная тайна»?
32. Какие сведения не подлежат засекречиванию?
33. Что такое засекречивание сведений и их носителей?
34. Каковы принципы засекречивания информации?
35. Какие степени секретности установлены Законом «О государственной тайне»?
36. Что такое допуск к государственной тайне?
37. Перечислите социальные гарантии, установленные для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе.
38. Перечислите основания для отказа гражданину в допуске государственной тайне.
39. Перечислите основания прекращения допуска к государственной тайне.
40. Что понимается под термином «персональные данные»?
41. Какими нормативными документами регулируются вопросы защиты персональных данных?
42. Раскройте содержание основных категорий персональных данных?
43. Что понимается под термином «информация, составляющая служебную тайну»?
44. Какими нормативными документами регулируются вопросы защиты служебной тайны?

45. Что понимается под термином «информация, составляющая коммерческую тайну»?

46. Какими нормативными правовыми документами регулируются вопросы защиты коммерческой тайны?

47. Какие сведения не могут составлять коммерческую тайну?

48. Что относится к мерам по обеспечению конфиденциальности информации, составляющей коммерческую тайну?

49. Какая информация относится к категории профессиональная тайна?

50. Приведите характеристику банковской тайны как вида защищаемой информации.

51. Приведите характеристику врачебной тайны как вида защищаемой информации.

52. Приведите характеристику адвокатской тайны как вида защищаемой информации.

53. Приведите характеристику нотариальной тайны как вида защищаемой информации.

54. Приведите характеристику тайны страхования как вида защищаемой информации.

55. Приведите характеристику тайны усыновления и тайны исповеди как видов защищаемой информации.

56. Что понимается под термином «интеллектуальная собственность»?

57. Какими нормативными документами регулируются вопросы интеллектуальной собственности?

58. Что относится к результатам интеллектуальной собственности?

59. Что такое авторское право?

60. Каковы особенности защиты программ для ЭВМ и баз данных институтом авторского права?

61. Что такое патентное право?

62. Перечислите объекты патентного права.

63. Приведите составы преступлений в области информационной безопасности, предусмотренные УК РФ.

64. Приведите составы правонарушений, предусмотренные КоАП РФ.

65. Дайте определение системы обеспечения информационной безопасности.

66. Перечислите задачи государственных органов в рамках деятельности по обеспечению информационной безопасности.

67. Перечислите задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности.

68. Что составляет организационную основу системы обеспечения информационной безопасности?

69. Перечислите полномочия Совета Федерации Федерального Собрания Российской Федерации в сфере обеспечения информационной безопасности.

70. Перечислите полномочия Государственной Думы Федерального Собрания Российской Федерации в сфере обеспечения информационной безопасности.

71. Перечислите полномочия Совета безопасности Российской Федерации в сфере обеспечения информационной безопасности.

72. Назовите функции Правительства Российской Федерации в области информационной безопасности.

73. Охарактеризуйте состав Межведомственной Комиссия по защите государственной тайны.

74. Полномочия Федеральной службы по техническому и экспортному контролю в сфере обеспечения информационной безопасности Российской Федерации.

75. Полномочия ФСБ России в сфере обеспечения информационной безопасности Российской Федерации.

76. Полномочия СВР России в сфере обеспечения информационной безопасности Российской Федерации.

77. Полномочия ФСО России в сфере обеспечения информационной безопасности Российской Федерации.

78. Полномочия Роскомнадзора в сфере обеспечения информационной безопасности Российской Федерации.

79. Охарактеризуйте понятия «лицензия» и «лицензирование».

80. Какие виды деятельности относятся к лицензируемым в сфере обеспечения информационной безопасности.

81. Перечислите полномочия Правительства Российской Федерации в области лицензирования.

82. Какие федеральные органы исполнительной власти относятся к лицензирующим органам в области информационной безопасности?

83. Что составляет систему нормативных правовых актов, регламентирующих деятельность лицензионных органов в области обеспечения информационной безопасности?

84. Какие документы составляют законодательную базу сертификации средств защиты информации?

3.5. Перечень тем докладов

1. Информационная безопасность Российской Федерации: вчера, сегодня, завтра.
2. Обеспечение информационной безопасности как приоритетное направление государственной политики Российской Федерации.
3. Основные угрозы личности в информационной сфере.
4. Основные угрозы общества в информационной сфере.
5. Основные угрозы государства в информационной сфере.
6. Информационная война как угроза информационной безопасности.
7. Защита информации и защита от информации на современном этапе развития Российской Федерации.
8. Информационное воздействие как угроза информационной безопасности Российской Федерации.
9. Место и роль правового направления в системе обеспечения информационной безопасности Российской Федерации.
10. Конституция РФ о правах и свободах человека и гражданина в информационной сфере.
11. Международно-правовой опыт защиты информации (на примере любого государства по выбору студента).
12. Исторические этапа развития законодательства в области обеспечения информационной безопасности.
13. Приоритетные направления развития законодательства в области обеспечения информационной безопасности.
14. Банковская тайна как вид защищаемой информации.
15. Врачебная тайна как вид защищаемой информации.
16. Адвокатская тайна как вид защищаемой информации.
17. Нотариальная тайн как вид защищаемой информации.
18. Тайна страхования как вид защищаемой информации.
19. Тайна усыновления как вид защищаемой информации.

20. Нормы международного права в области защиты интеллектуальной собственности.
21. История развития законодательства в области защиты интеллектуальной собственности.
22. Гражданско-правовая ответственность за нарушения в области интеллектуальной собственности.
23. Административная ответственность за нарушения в области интеллектуальной собственности.
24. Уголовная ответственность за нарушения в области интеллектуальной собственности
25. Информация как объект противоправного воздействия.
26. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации как новый вид преступного посягательства.
27. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.
28. Правонарушения в области патентных и авторских прав.
29. Мошенничество в сфере компьютерной информации.
30. Мошенничество с использованием платежных карт.
31. Неправомерное использование инсайдерской информации.
32. Уголовная ответственность в области защиты государственной тайны.
33. Юридическая ответственность в области защиты персональных данных субъекта.
34. Виды деятельности в области защиты информации, подлежащие обязательному лицензированию.
35. Организационная структура системы сертификации в области защиты информации.
36. Административная отвесность за правонарушения в сфере лицензирования и сертификации.

3.6 Типовые практические задачи

Для решения задач рекомендуется использовать справочную правовую систему Гарант, справочную правовую систему Консультант Плюс, профессиональные справочные системы «Кодекс».

Задача 1. Из действующих нормативных правовых актов приведите не менее трех примеров информационно-правовых норм следующих классификаций:
- обязывающие, управомачивающие, запрещающие;
- материальные и процессуальные;
- нормы, закрепляющие права граждан на информацию;
- нормы, устанавливающие обязанность органов государственного управления предоставлять информацию физическим и юридическим лицам.

Задача 2. Приведите по два примера источников права в области информационной безопасности:
- Акты международного права;
- Федеральные законы;
- Указы Президента РФ;
- Постановления Правительства РФ;
- Акты федеральных органов исполнительной власти;
- Законы субъектов РФ.

Задача 3. Раскройте сущность понятий: защищаемая информация, информация с ограниченным доступом, конфиденциальная информация, тайна и постройте схему их соотношения.

Задача 4. Заполните таблицу:

№ п/п	Вид информации с ограниченным доступом	Понятие	Правовое регулирование	Обладатель	Субъект защиты	Нормы юридической ответственности

Задача 5. Вставьте в предложение пропущенные слова:

- «государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, … Российской Федерации»;
- «основными принципами отнесения сведений к государственной тайне и их засекречивания являются принципы …»;
- «в ст. 8 Закона «О государственной тайне» установлены …»;
- «разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится … без …такой информации либо вопреки трудовому или гражданско-правовому договору»;
- «обезличивание персональных данных - действия, в результате которых становится … информации определить … персональных данных … персональных данных».

Задача 6. Соотнесите термин и содержание его понятия:

Термин	Содержание понятия
1. персональные данные	1. государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
2. блокирование персональных данных	2. действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
3. оператор персональных данных	3. действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
4. распространение персональных данных	4. действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
5. уничтожение персональных данных	5. временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)

6. биометрические персональные данные	6. любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
7. трансграничная передача персональных данных	7. сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность
8. предоставление персональных данных	8. передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

Задача 7. В 2018 году сотрудник отдела кадров УМВД России по Брянской области Н.И. Гвоздова произвела копирование 10 документов с пометкой «Для служебного пользования», находящихся на данный период у нее в производстве, для использования в работе в качестве образцов. В 2019 году вышеуказанные документы были обнаружены при досмотре личного автотранспорта в багажнике ее автомобиля. Какая ответственность предусмотрена за данное нарушение? Будет ли привлекаться к ответственности по условию задачи Н.И. Гвоздова? Ответ мотивируйте ссылкой на законодательство.

Задача 8. Работник архивного фонда Российской Федерации Буханин в публикациях в средствах массовой информации использовал известные ему по службе сведения, касающиеся научно-технических разработок (1985-1987 г.г.) НИИ «Вермос». Сведения относились к государственной тайне, однако Буханин сослался в публикации на то, что прошло много лет со времени событий, описываемых им в публикации, и народ должен знать такие факты. Дайте правовую оценку действиям Буханина.

Задача 9. Руководитель фирмы «Наше зерно» Востриков поручил сотруднику этой фирмы Иванову временно устроиться на работу в конкурирующую фирму «Золотое поле» и выяснить перспективные планы ее коммерческой деятельности, а также заполучить документацию, касающуюся фирмы «Золотое поле». Иванов был принят на работу в фирму, выяснил все ее коммерческие тайны и передал их Вострикову, за что получил крупное денежное вознаграждение. Фирма «Наше зерно», воспользовавшись полученной информацией, завоевала доминирующее положение на рынке сбыта зерна, что привело к банкротству фирмы «Золотое поле». Прокомментируйте поведение указанных в задаче лиц.

Задача 10. За опубликование редакцией газеты «Сегодня» материалов, которые содержали персональные данные несовершеннолетней гражданки, а именно фамилии, имени, сведений о школе, в которой обучается несовершеннолетняя, без ее согласия и согласия ее законного представителя, а также ряда других статей с персональными данными несовершеннолетних, Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций вынесло письменное предупреждение о недопустимости распространения через средство массовой информации сведений, составляющих специально охраняемую законом тайну, главному редактору СМИ газеты «Сегодня». Однако, главный редактор не отреагировала на это предупреждение и продолжал публиковать персональные данные граждан без их согласия. Поэтому Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций обратилось в Воронежский областной суд с исковым заявлением о прекращении деятельности газеты «Сегодня». Какое решение, по Вашему мнению, примет суд?

Задача 11. Укажите не менее трех отличий между режимами:

- служебной тайны и коммерческой тайны;
- служебной тайны и врачебной тайны;
- банковской тайны и персональных данных.

Задача 12. Соотнесите термин и содержание его понятия:

Термин	Содержание понятия
1. авторское право	1. подотрасль гражданского права, регулирующая правоотношения, связанные с созданием и использованием (изготовление, применение, продажа, иное введение в гражданский оборот) объектов интеллектуальной собственности, охраняемых патентом.
2. интеллектуальная собственность	2. результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (результаты интеллектуальной деятельности и средства индивидуализации)
3. интеллектуальные права	3. совокупность правовых норм, регулирующих отношения, возникающие между объектами и субъектами права в отношении созданного произведения.
4. патентное право	4. список результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, которым предоставляется правовая защита

Задача 13. Выберите из приведенного ниже перечня объекты авторского права:

1) произведения науки, литературы и искусства;
2) программы для электронных вычислительных машин (программы для ЭВМ);
3) базы данных;
4) исполнения;
5) фонограммы;
6) сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
7) изобретения;
8) полезные модели;
9) промышленные образцы;
10) селекционные достижения;
11) топологии интегральных микросхем;
12) секреты производства (ноу-хау);
13) фирменные наименования;
14) товарные знаки и знаки обслуживания;
15) наименования мест происхождения товаров;
16) коммерческие обозначения.

Задача 14. Определите срок действия авторского права на произведение, созданное:

- одним автором в 2010 г.;
- двумя авторами в 2015 г.;
- анонимно в 2017 г.

Задача 15. Петров И.И., являясь доцентом кафедры уголовного права разработал и издал «Практикум по дисциплине «Уголовное право»», предназначенный для студентов, обучающихся по юридическим специальностям. Определите, какими правами будет обладать Петров И.И.

Задача 16. Заполните таблицу «Объекты патентных прав».

№ п/п	Наименование объекта патентных прав	Понятие объекта	Показатели патентоспособности	Наименование документа, подтверждающего	Срок действия документа, возможность

				наличие прав	продления
1.	изобретение				
2.	полезная модель				
3.	промышленный образец				

Задача 17. Соотнесите понятия: «информационное правонарушение», «информационное преступление», «компьютерное преступление». Ответ обоснуйте.

Задача 18. Тождественны ли понятия «компьютерное преступление» и «преступление в сфере высоких технологий»? Ответ обоснуйте.

Задача 19. Приведите по одному примеру (в соответствии с нормами законодательства) преступлений в области информационной безопасности, в частности:

- против свободы массовой информации;
- против реализации права на поиск, получение и передачу информации;
- в отношении сведений, составляющих государственную тайну;
- в отношении сведений конфиденциального характера;
- в сфере защиты и обработки персональных данных;
- посягающие на личную тайну;
- направленные на распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию;
- направленные против безопасного обращения компьютерной информации, которые посягают на интересы личности и общества в сфере информационного обмена, создания, защиты, хранения и использования информации, хранящейся в компьютере.

Задача 20. Сотрудник фирмы «Сибинтек» Левченко, пользуясь правами администратора сетей и имея доступ к содержащейся на персональном компьютере информации, самовольно скопировал на носитель информации сведения, составляющие коммерческую тайну. После своего увольнения Левченко передал полученную таким образом информацию директору конкурирующей фирмы, получив при этом вознаграждение 10 тыс. евро. Дайте юридическую оценку описанным действиям.

Задача 21. Выпускник факультета прикладной механики и математики ВУЗа Иванов, имея навыки программирования, создал компьютерную программу, которая выполняла следующие функции: действуя в компьютерной сети банка она переводила денежные средства в различных размерах в случайном порядке со счетов одних клиентов банка на счета других, в том числе и на счет Иванова, открытый им заблаговременно. Эта программа была внедрена другом Иванова Бурчатовым, работающим в коммерческом банке «Восток». Денежные средства получить в ходе проведенных действий не удалось благодаря своевременному вмешательству службы безопасности банка, однако деятельность банка в результате сбоя компьютеров была парализована на 3 дня. Дайте юридическую оценку описанным действиям.

Задача 22. Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы. Дайте юридическую оценку описанным действиям.

Задача 23. Аспирант университета Хохлов, 23-ти лет, занимался исследовательской работой по компьютерной "вирусологии". Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые "сетевые черви", проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью

уничтожены списки сотрудников универ-ситета, расчеты бухгалтерии по зарплате, повреждены материалы науч-но-исследовательской работы, в том числе "пропали" две кандидатские и одна докторская диссертации. Дайте юридическую оценку описанным действиям.

Задача 24. Левченко и другие граждане Российской Федерации вступили в сговор на похищение денежных средств в крупных размерах, принадлежащих "City Bank of America", расположенного в г. Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 2012 г., используя электронную компьютерную систему телекоммуникационной связи "Интернет" и преодолев при этом несколько рубежей многоконтурной защиты от несанкционированного доступа с помощью персонального компьютера стандартной конфигурации из офиса предприятия, находящегося в г. Санкт-Петербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате этих операций было осуществлено не менее 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка на счета лиц, входящих в состав преступной группы, проживающих в шести странах: США, Великобритании, Израиле, Швейцарии, ФРГ, России. Дайте уголовно-правовую оценку действиям Левченко и других членов организованной группы.

Задача 25. Составьте схему элементов структуры государственной системы обеспечения информационной безопасности РФ.

Задача 26. На основе законодательства и подзаконных нормативных правовых актов назовите федеральные органы исполнительной власти, входящие в государственную систему обеспечения информационной безопасности. Заполните таблицу.

№ п/п	Наименование федерального органа исполнительной власти	Полномочия в области обеспечения информационной безопасности	Правовая основа деятельности

Задача 27. На основе законодательства и подзаконных нормативных правовых актов составьте таблицу «Система лицензирования в области защиты информации», в которой необходимо отразить участников системы лицензирования, их полномочия и правовую основу деятельности. Заполните таблицу:

№ п/п	Участник системы лицензирования	Полномочия	Правовая основа
1.			
2.			

Задача 28. На основе законодательства и подзаконных нормативных правовых актов назовите виды деятельности в области защиты информации, подлежащие лицензированию и субъекты, осуществляющие лицензирование этих видов деятельности. Заполните таблицу:

№ п/п	Вид деятельности	Субъект, осуществляющий лицензирование	Правовая основа
1.			
2.			
3.			

Задача 29. Постройте алгоритм действий соискателю на получение лицензии на занятие деятельностью по разработке и производству средств защиты конфиденциальной информации.

Задача 30. Постройте алгоритм действий на получение сертификата на средство защиты конфиденциальной информации.

Задача 31. На основе законодательства и подзаконных нормативных правовых актов назовите виды продукции в области защиты информации, подлежащие сертификации и субъекты, осуществляющие их сертификацию. Заполните таблицу:

№ п/п	Вид продукции	Субъект, осуществляющий сертификацию	Правовая основа
1.			
2.			
3.			

Задача 32. 12.09.2019 года в ходе осуществления контроля за состоянием информационной безопасности на базе комплексного хранения (г.Воронеж), на ПЭВМ (уч.№ 553), установленных в помещении №27 базы, выявлен факт использования несертифицированных для Министерства обороны РФ систем Microsoft Windows7 Максимальная. Данное СВТ используется для обработки информации, составляющей государственную тайну. Дайте юридическую оценку выявленному факту. Кто уполномочен осуществлять контроль за состоянием информационной безопасности. Кто рассматривает данное правонарушение.

Задача 33. В Центральный районный суд г. Воронежа поступил административный материал в отношении ООО ЧОП «Планета», из протокола об административном правонарушении следует, что 17.11.2019 работник ЧОП «Планета» К. использовал поисковый комплекс путем надевания наушников, включил прибор и ходил, выявлял подслушивающие технические средства внутри помещения, т.е. осуществлял деятельность без соответствующего разрешения и лицензии согласно п. 3 ст.12 ФЗ «о лицензировании отдельных видов деятельности от 04.05.2011 года, т.е. совершил административное правонарушение предусмотренное ст. 13.13 ч. 2 Кодекса РФ об административных правонарушениях.

В судебном заседании директор ООО ЧОП «Планета» Б. вину в совершении данного административного правонарушения не признал, пояснил, что ЧОП «Планета» создан в 2007 году, с 2007 года он является директором, К. работает на предприятии инженером по техники безопасности. В ноябре 2019 года они приобрели оборудование – спектральный коррелятор и нелинейный локатор для обеспечения собственных нужд их предприятия ЧОП «Экстрим», тогда же в ноябре 2019 года К. был направлен на курсы, где прошел обучение по работе с данными приборами для использования данных приборов для собственных нужд предприятия. С ноября 2019 года ЧОП «Планета» никаких услуг с применением данных приборов ни физическим лицам, ни юридическим лицам не оказывало, никаких заявлений, договоров на оказание таких услуг не имеется. 17.11.2019 года К. обратился к нему с просьбой показать приборы руководителю иной подобной организации, так как те также хотели приобрести аналогичные приборы, он разрешил К. показать их, никакой деятельности с применением этих приборов ЧОП «Планета» не проводило.

Какое решение, по Вашему мнению, примет суд. Свой ответ аргументируйте.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

4.1. Положение о формах, периодичности и порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся:

Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся П ВГАУ 1.1.01 – 2017,

Положение о фонде оценочных средств П ВГАУ 1.1.13 – 2016

4.2. Методические указания по проведению текущего контроля

1.	Сроки проведения текущего контроля	На семинарах
2.	Место и время проведения текущего контроля	В учебной аудитории в течение семинара
3.	Требования к техническому оснащению аудитории	В соответствии с ОП и рабочей программой
4.	Ф.И.О. преподавателя (ей), проводящих процедуру контроля	Филиппова Н.В.
5.	Вид и форма заданий	Собеседование, письменные работы
6.	Время для выполнения заданий	в течение занятия
7.	Возможность использований дополнительных материалов.	Обучающийся может пользоваться дополнительными материалами
8.	Ф.И.О. преподавателя, обрабатывающих результаты	Филиппова Н.В.
9.	Методы оценки результатов	Экспертный
10.	Предъявление результатов	Оценка выставляется в журнал и доводится до сведения обучающихся в конце занятия
11.	Апелляция результатов	В порядке, установленном нормативными документами, регулирующими образовательный процесс в Воронежском ГАУ

4.3 Ключи (ответы) к контрольным заданиям, материалам, необходимым для оценки знаний

Находятся на кафедре у преподавателя, осуществляющего процедуру контроля