МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
технологий обработки и защиты информации

А.А. Сирота

23.12.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.49 Организационное и правовое обеспечение информационной безопасности

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Разработка защищенного программного обеспечения

3. Квалификация выпускника: Специалитет

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Филиппова Неля Викторовна, к.ю.н, доцент

7. Рекомендована: научно-методическим советом ФКН, протокол № 3 от 22.11.2023 г.

8. Учебный год: 2025-2026 **Семестр(ы)/Триместр(ы):** 4

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:
формирование у обучающихся знаний, умений и навыков в сфере организационного и правового обеспечения информационной безопасности.
Задачи дисциплины:

- овладение обучающимися системными знаниями правовых основ обеспечения информационной безопасности;
- сформировать у обучающихся с помощью практических заданий и других форм активного обучения, устойчивые умения и компетенции, способствующие правильному применению правовых и организационных методов обеспечения информационной безопасности;
- формирование у обучающихся высокого уровня правосознания и правовой культуры в области информационной безопасности, обеспечивающих неукоснительное соблюдение действующего законодательства и руководящих документов;
- сформировать навыки, умения и компетенции изучения нормативных правовых документов в области защиты информации;
- формирование навыков по разработке предложений по совершенствованию и повышению эффективности комплекса мер по обеспечению информационной безопасности телекоммуникационной системы;
- способность организация работ по выполнению требований режима защиты информации ограниченного доступа;
- формирование умения разработки методических материалов и организационно-распорядительных документов по обеспечению информационной безопасности телекоммуникационных систем на предприятиях.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относиться к обязательной части Блок 1. Дисциплины (модули).

Входные знания в области основ информационной безопасности.

Дисциплина является предшествующей для дисциплины «Техническая защита информации».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.3	умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	Уметь: применять нормативные правовые акты, нормативные и методические документы, регламентирующие защиту сведений, составляющих государственную тайну и иных сведений ограниченного доступа Владеть: навыками работы с нормативными правовыми актами; навыками анализа нормативных правовых документов в области обеспечения информационной безопасности; навыками отнесения информации к различным видам и степеням конфиденциальности
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламен-	ОПК-5.5	знает основы: российской правовой системы и законодательства, правового статуса личности, органи-	Знать: основы правового обеспечения информационной безопасности; основные положения законодательства РФ в области информационной безопасности права, свободы и обязанности личности в области информационной безопасности;

	тирующие деятельность по защите информации;		зации и деятельности органов государственной власти в Российской Федерации;	организационную структуру государственной системы обеспечения информационной безопасности РФ Уметь: применять действующую законодательную базу в области обеспечения безопасности информации; осуществлять поиск необходимых нормативных правовых актов и отдельных информационно-правовых норм в системе действующего законодательства, в том числе с помощью справочно-поисковых систем правовой информации.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.6	знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации;	Знать: основные категории, понятия, положения отраслевого законодательства, регулирующего сферу информационной безопасности Уметь: оперировать основными категориями, понятиями, положениями отраслевого законодательства, регулирующего сферу информационной безопасности; применять положения отраслевого законодательства в области обеспечения безопасности информации; осуществлять поиск необходимых норм отраслевого законодательства.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.7	знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;	Знать: понятие и виды защищаемой информации; основные положения законодательства Российской Федерации, нормативных правовых актов, нормативных и методических документов в области обеспечения безопасности государственной тайны и иных видов информации ограниченного доступа; организационные основы обеспечения безопасности государственной тайны и иных видов информации ограниченного доступа; характеристику преступлений и иных видов правонарушений в сфере информационной безопасности; меры юридической ответственности за правонарушения в области информационной безопасности. Уметь: осуществлять поиск необходимых положений законодательства Российской Федерации, нормативных правовых актов, нормативных и методических документов в области обеспечения безопасности государственной тайны и иных видов информации ограниченного доступа.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.8	знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;	Знать: место персональных данных в системе информации ограниченного доступа, категории и понятия в области безопасности персональных данных, основные положения нормативных правовых актом и методических документов, регламентирующих защиту персональных данных; основы правового регулирования охраны результатов интеллектуальной деятельности.

				Уметь: осуществлять поиск необходимых положений нормативных правовых актов и методических документов в области обеспечения безопасности персональных данных и охраны результатов интеллектуальной деятельности.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.9	умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;	Уметь: осуществлять поиск необходимых положений нормативных правовых актов и методических документов в области обеспечения безопасности информации и их анализ; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, положениями действующего законодательства, нормативных правовых и методических документов; предпринимать необходимые меры по восстановлению нарушенных прав. Владеть: системным подходом к организации безопасности информации; навыками работы с нормативными правовыми актами; навыками анализа нормативных правовых документов в области обеспечения информационной безопасности; навыками обоснования решений, связанных с реализацией правовых норм по защите информации в пределах должностных обязанностей, положениями действующего законодательства, нормативных правовых и методических документов; навыками реализации необходимых мер по восстановлению нарушенных прав.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.10	умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;	Уметь: разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций, а также проводить анализ разработанных проектов; Владеть: навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций, а также их анализа;
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.11	умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и атте-	Уметь: формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций

			стации по требованиям безопасности информации;	Владеть: навыками определения требований при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.12	умеет формулировать основные требования информационной безопасности при эксплуатации компьютерной системы;	Уметь: формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; Владеть: навыками определения требований информационной безопасности при эксплуатации компьютерной системы
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.13	умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;	Уметь: формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций Владеть: навыками определения требований по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1	знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	Знать: положения нормативных правовых актов, регламентирующих деятельность по лицензированию в области обеспечения защиты государственной тайны, технической защите конфиденциальной информации, по аттестации объектов информатизации и сертификации Уметь: применять положения нормативных правовых актов, регламентирующих деятельность по лицензированию в области обеспечения защиты государственной тайны, технической защите конфиденциальной информации, по аттестации объектов информатизации и сертификации
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.2	знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях;	Знать: положения нормативных правовых актов, нормативных и методических документов ФСБ России, ФСТЭК России, задачи и их полномочия в области обеспечения безопасности информации; задачи и полномочия служб защиты информации на предприятия Уметь: применять положения нормативных правовых актов, нормативных и методических документов ФСБ России, ФСТЭК России при реализации задач и полномочий служб защиты информации на предприятия

ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.3	знает систему организационных мер, направленных на защиту информации ограниченного доступа	Знать: основы организационного обеспечения информационной безопасности; организационные меры защиты информации ограниченного доступа; Уметь: применять организационные меры защиты информации ограниченного доступа;
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.4	знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа	Знать: положения нормативных правовых актов, нормативных и методических документов ФСБ России, ФСТЭК России по защите информации ограниченного доступа Уметь: применять положения нормативных правовых актов, нормативных и методических документов ФСБ России, ФСТЭК России при реализации задач и полномочий по защите информации ограниченного доступа
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.5	знает основные угрозы безопасности информации и модели нарушителя компьютерных систем;	Знать: понятие, классификации угроз безопасности информации и модели нарушителя компьютерных систем Уметь: определять основные угрозы безопасности информации и модели нарушителя компьютерных систем.
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми	ОПК-6.6	умеет разрабатывать модели угроз и модели нарушителя компьютерных систем;	Уметь: определять основные угрозы безопасности информации и разрабатывать модели угроз и модели нарушителя компьютерных систем; Владеть: навыками определения основных угроз безопасности информации и разработки модели угроз и модели нарушителя компьютерных систем

	актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;			
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.7	умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	Уметь: разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Владеть: навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.8	умеет определить политику контроля доступа работников к информации ограниченного доступа	Уметь: определить политику контроля доступа работников к информации ограниченного доступа на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Владеть: определения политики контроля доступа работников к информации ограниченного доступа
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.9	умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	Уметь: формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Владеть: навыками определения основных требований, предъявляемых к физической защите объекта и пропускному режиму в организации

ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.10	умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	Уметь: применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; Владеть: навыками применения отечественных и зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы

12. Объем дисциплины в зачетных единицах/час. — 2/72.

Форма промежуточной аттестации: зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра - 4	№ семестра	итого
Аудиторные занятия		72	72		72
в том числе:	лекции	16	16		16
	практические	32	32		32
	лабораторные				
Самостоятельная работа		24	24		24
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачет с оценкой)*					
Итого:		72	72		72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Информационная безопасность как определяющий компонент национальной безопасности РФ. Законодательство в области обеспечения информационной безопасности	Место информационной безопасности в системе национальной безопасности РФ. Понятие, структура и содержание информационной безопасности. Угрозы информационной безопасности личности, обществу и государству. Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства, современных автоматизированных и телекоммуникационных систем. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ.	
1.2	Информация как объект правового регулирования	Информация как объект правоотношений в сфере обеспечения информационной безопасности. Информация и информационные системы – объекты	

		правоотношений в сфере обеспечения информационной безопасности. Понятие и виды защищаемой информации.	
1.3	Правовое регулирование информационной безопасности в сфере интеллектуальной собственности	Защита интеллектуальной собственности в системе правового регулирования информационной безопасности. Основы авторского права. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем. Особенности правовой охраны программ для ЭВМ и баз данных. Особенности правовой охраны топологий интегральных микросхем.	
1.4	Правонарушения в сфере защиты информации	Юридическая ответственность за нарушение правовых норм защиты информации. Понятие юридической ответственности за нарушение правовых норм в области информационной безопасности. Виды юридической ответственности за нарушение правовых норм в области информационной безопасности. Характеристика отдельных видов юридической ответственности в сфере защиты информации.	
1.5	Государственная система обеспечения информационной безопасности	Понятие и задачи государственной системы обеспечения информационной безопасности в РФ. Структура государственной системы информационной безопасности в РФ. Организационная основа системы информационной безопасности РФ. Функции элементов организационной основы системы информационной безопасности РФ.	
1.6	Системы лицензирования и сертификации в области защиты информации	Система лицензирования в области защиты информации. Основные понятия и положения системы государственного лицензирования. Организационная структура системы государственного лицензирования. Система сертификации в области защиты информации. Основные понятия и система сертификации продукции и услуг.	
1.7	Аттестация объектов информатизации по требованиям безопасности информации	Аттестация объектов информатизации по требованиям безопасности информации. Основные положения аттестации объектов информатизации по требованиям безопасности информации.	
1.8	Организационно-техническое обеспечение защиты информации на объектах информатизации	Основные понятия и положения технической защиты информации. Организационно-технические мероприятия по защите информации.	
2. Практические занятия			
2.1	Информационная безопасность как определяющий компонент национальной безопасности РФ. Законодательство в области обеспечения информационной безопасности	Понятие и содержание правового обеспечения информационной безопасности. Классификация и структура нормативных правовых актов в сфере обеспечения защиты информации. Конституция и гражданский кодекс РФ о правах и обязанностях граждан России в сфере обеспечения информационной безопасности. Международно-правовой опыт защиты информации. Международно-правовые нормы в области защиты информации. Международное сотрудничество в области борьбы с преступностью в сфере высоких технологий. Содержание основных законодательных актов сфере информационной безопасности. Основные положения Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Основные положения Федерального закона от 27 декабря 2002г. №184-ФЗ «О техническом регулировании». Правовые основы деятельности в области связи. Правовое регулирование отношений в области использования электронных подписей.	

2.2	Информация как объект правового регулирования	Государственная тайна как особый вид защищаемой информации. Правовая основа обеспечения защиты государственной тайны. Организация защиты государственной тайны. Правовая основа защиты отдельных видов конфиденциальной информации. Правовая основа обеспечения защиты коммерческой тайны. Правовое обеспечение защиты служебной тайны. Персональные данные как вид защищаемой конфиденциальной информации. Понятие и виды персональных данных. Правовая основа обеспечения защиты персональных данных. Правовая основа защиты профессиональных тайн. Банковская тайна как вид защищаемой информации. Врачебная тайна как вид защищаемой информации. Адвокатская тайна как вид защищаемой информации. Нотариальная тайн как вид защищаемой информации. Тайна страхования как вид защищаемой информации. Тайна усыновления и тайна исповеди как виды защищаемой информации.	
2.3	Правовое регулирование информационной безопасности в сфере интеллектуальной собственности	Защита объектов промышленной собственности на основе патентов. Основные положения патентного права. Организационно-правовая система обеспечения защиты объектов промышленной собственности на основе патентов.	
2.4	Правонарушения в сфере защиты информации	Уголовная ответственность за нарушение правовых норм в сфере за-щиты информации. Административная ответственность за нарушения правовых норм в сфере защиты информации. Особенности юридической ответственности за нарушения норм защиты информации в области трудовых и гражданско-правовых отношений. Уголовно-правовая ответственность за противоправные действия в сфере защиты информации. Уголовная ответственность за нарушение правовых норм, предусмотренных главой 28 УК РФ. Уголовная ответственность за нарушение правовых норм, предусмотренных главой 29 УК РФ.	
2.5	Государственная система обеспечения информационной безопасности	Методы организационной защиты информации. Формы организационной защиты информации. Методы обеспечения физической безопасности. Место физической безопасности в обеспечении комплексной защиты информации. Содержание методов обеспечения физической безопасности. Организация пропускного и внутриобъектового режимов. Режим хранения носителей конфиденциальной информации. Классификация помещений в зависимости от условий доступа. Основные меры по обеспечению сохранности носителей конфиденциальной информации.	
2.6	Системы лицензирования и сертификации в области защиты информации	Особенности сертификации средств защиты информации. Ответственность за правонарушения в сфере лицензирования и сертификации. Особенности лицензирования и сертификации в области защиты информации. Организационные аспекты получения лицензии на занятие определенным видом деятельности в сфере обеспечения информационной безопасности. Организационные аспекты получения сертификата соответствия на средства защиты информации.	
2.7	Аттестация объектов информатизации по требованиям безопасности информации	Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.	

2.8	Организационно-техническое обеспечение защиты информации на объектах информатизации	Технические средства, используемые в рамках обеспечения информационной безопасности	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Информационная безопасность как определяющий компонент национальной безопасности РФ. Законодательство в области обеспечения информационной безопасности	2	2		2	6
2	Информация как объект правового регулирования	2	6		2	10
3	Правовое регулирование информационной безопасности в сфере интеллектуальной собственности	2	2		2	6
4	Правонарушения в сфере защиты информации	2	2		2	6
5	Государственная система обеспечения информационной безопасности	2	4		2	8
6	Системы лицензирования и сертификации в области защиты информации	2	8		4	14
7	Аттестация объектов информатизации по требованиям безопасности информации	2	4		4	10
8	Организационно-техническое обеспечение защиты информации на объектах информатизации	2	4		6	12
	Итого:	16	32		24	72

14. Методические указания для обучающихся по освоению дисциплины: 1) При освоении дисциплины рекомендуется использовать следующие средства:

- изучение рекомендуемой основной и дополнительной литературы методических указаний и пособий;
- работа с текстом конспекта лекций;
- систематическая подготовка к практическим занятиям;
- выполнение контрольных заданий для закрепления теоретического материала;
- работа с электронными версиями учебников и методических указаний для выполнения лабораторно-практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и лабораторных работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	*Ажмухамедов, И. М. Основы организационно-правового обеспечения информационной безопасности : учебное пособие / И. М. Ажмухамедов, О. М. Князева. — Санкт-Петербург : Интермедия, 2017. — 264 с. — ISBN 978-5-4383-0160-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103196 (дата обращения: 30.06.2021). — Режим доступа: для авториз. пользователей.*
2	*Мельников, Владимир Павлович. Информационная безопасность : [учебник для студ. вузов, обучающихся по направлениям подготовки "Конструкторско-технологическое обеспечение машиностроительных производств", "Автоматизация технологических процессов и производств"] / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева ; под ред. В.П. Мельникова .— 2-е изд., перераб. и доп. — Москва : КноРус, 2018 .— 371 с. : ил., цв. ил., табл. — (Бакалавриат) .— Библиогр.: с. 369-371.*

б) дополнительная литература:

№ п/п	Источник
1	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры: [для студентов высших учебных заведений, обучающихся по юридическим направлениям и специальностям] / под ред. Т.А. Поляковой, А.А. Стрельцова .— Москва : Юрайт, 2018 .— 324, [1] с. : ил. — (Бакалавр и магистр. Академический курс) .— Библиогр.: с. 324-[325].
2	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— Москва : ACADEMIA, 2006 .— 330 с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с. 327-328.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1	ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024)
2	ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024)
3	ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025)
4	Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027)
5	ЭБС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025)

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
	Справочно-информационная система «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используются:

1. ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.

2.При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru),

базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 477
Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479
Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19", мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 505п
Учебная аудитория: специализированная мебель, компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17", мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 292
Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для ви-деоконференций Logitech ConferenceCam
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380
Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17", мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 305п
Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 307п
Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

Перечень программного обеспечения, используемого в образовательном процессе

№ пп	Наименование ПО	Производитель ПО (или торговая марка, Или правообладатель) при наличии
	ОС Windows v.7, 8, 10	Microsoft (прим. 1)
2	СУБД Oracle Database 11g Express Edition	Oracle
3	Microsoft Visio, Access, OneNote v. 2010-2019	Microsoft
4	Visual Studio, v. 2010-2019	Microsoft
5	Набор утилит (архиваторы, файл-менеджеры)	GNU, BSD
6	ОС GNU/Linux (CentOS) v.6-8	RedHat, GNU

7	LibreOffice v.5-7	The Document Foundation, GNU
8	Среда разработки Eclipse	Eclipse Foundation
9	GlassFish Java EE	Eclipse Foundation
10	Python ver 3.8	Python Software Foundation
11	MySQL Workbench Community	GNU
12	PyCharm Community	JetBrains
13	IntelliJ IDEA	JetBrains
14	Среда разработки NetBeans IDE	ORACLE
15	Дистрибутив Anaconda/Python	BSD
16	Системы моделрования системной Динамики Vensim	Ventana Systemms Inc.
17	Системы моделирования бизнес процессов BizAgi	BizAgi
18	Системы управления проектами Wrike	Wrike Inc.
19	Системы моделирования Modelio	Modeliosoft
20	MATLAB “Total Academic Headcount – 25”	MathWorks (прим. 2)
21	HUGIN EXPERT / HUGIN Lite (open-source)	HUGIN EXPERT A/S
22	Справочно-правовая система (СПС) Консультант+ для образования	Консультант+ (прим. 7)
23	Microsoft SQL Server	Microsoft
24	Packet Tracer	CISCO Systems
25	Virtual Box	ORACLE
26	Microsoft Windows Virtual PC	Microsoft
27	VLC media player	VideoLAN, GNU
28	Google Workspace for Education Fundamentals (ранее G Suite for Education и Google-Apps for Education)	Google Inc.
29	SecretNet Studio 8 (демоверсия)	ООО Код Безопасности
30	Dr. Web Enterprise Security Suite	Компания «Доктор Веб» (прим. 3)
31	XSpider	Компания Positive Technologies (прим. 4)
32	СКЗИ «КриптоПро Рутокен CSP»	Компания КриптоПро (прим. 5)
33	ViPNet	ОАО ИнфоТеКС (прим. 6)
34	ERwin Data Modeler Standard Edition	CA Technologies (лицензия до 2025 г., Contract#: 40217535)
35	Платформа электронного обучения LMS-Moodle, основа Образовательного портала «Электронный университет ВГУ»	Moodle Pty Ltd, GNU General Public License
36	PHP	PHP Group
37	Notepad++	GNU
38	PuTTY	MIT
39	Ramus Educational	Алексей Чижевский
40	ОС GNU/Linux (Ubuntu)	Canonical Ltd, GNU
41	Foxit PDF Reader	корпорация FOXIT SOFTWARE INC., проприетарная бесплатная лицензия
42	Операционная система РЕД ОС	ООО Ред Софт (прим. 9)
43	Система виртуализации РЕД Виртуализация	ООО Ред Софт (прим. 9)

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Информационная безопасность как определяющий компонент национальной безопасности РФ. Законодательство в области обеспечения информационной безопасности	ОПК-5	ОПК-5.3, ОПК-5.5, ОПК-5.6, ОПК-5.7, ОПК-5.9, ОПК-6.1	Устный опрос Тест № 1 Практическое задание
2.	Информация как объект правового регулирования	ОПК-5	ОПК-5.3, ОПК-5.5, ОПК-5.6, ОПК-5.7, ОПК-5.8, ОПК-5.8, ОПК-5.13	Устный опрос Тест № 2 Практическое задание
3.	Правовое регулирование информационной безопасности в сфере интеллектуальной собственности	ОПК-5	ОПК-5.6, ОПК-5.7, ОПК-5.8, ОПК-5.13	Устный опрос Тест № 3 Практическое задание
4.	Правонарушения в сфере защиты информации	ОПК-5	ОПК-5.6, ОПК-5.7, ОПК-5.9	Устный опрос Тест № 4 Практическое задание
5.	Государственная система обеспечения информационной безопасности	ОПК-5 ОПК-6	ОПК-5.5, ОПК-5.10, ОПК-6.1, ОПК-6.2, ОПК-6.3, ОПК-6.4; ОПК-6.5; ОПК-6.7;ОПК-6.9	Устный опрос Тест № 5 Практическое задание
6.	Системы лицензирования и сертификации в области защиты информации	ОПК-5 ОПК-6	ОПК-5.7, ОПК-5.10, ОПК-5.11, ОПК-5.12, ОПК-6.1, ОПК-6.4	Устный опрос Тест № 6 Практическое задание
7.	Аттестация объектов информатизации по требованиям безопасности информации	ОПК-5 ОПК-6	ОПК-5.9, ОПК-5.10, ОПК-5.12, ОПК-5.13, ОПК-6.1, ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.7; ОПК-6,8; ОПК-6.9, ОПК-6.10	Устный опрос Тест № 7 Практическое задание
8.	Организационно-техническое обеспечение защиты информации на объектах информатизации	ОПК-5 ОПК-6	ОПК-5.9, ОПК-5.10, ОПК-5.12, ОПК-5.13, ОПК-6.1, ОПК-6.2, ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.7; ОПК-6,8; ОПК-6.9, ОПК-6.10	Устный опрос Тест № 8 Практическое задание
Промежуточная аттестация форма контроля – зачет с оценкой				Комплект КИМ

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными;

3) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на зачете с оценкой

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Тест	Теоретические вопросы по темам/разделам дисциплины	Содержит 4 тестовых вопроса, за правильный ответ на каждый из которых дается 1 балл
3	Практическое задание	Практические задачи	Оценка «отлично» выставляется студенту, если он исчерпывающе и свободно справляется с практическими заданиями, дает правильное обоснование принятого решения; Оценка «хорошо» выставляется студенту, если он правильно, но недостаточно полно выполняет задания, не допускает существенных неточностей; Оценка «удовлетворительно» выставляется студенту, если он допускает неточности в ответе, испытывает затруднения в выполнении практических заданий, при указании на существенные ошибки может их исправить; Оценка «неудовлетворительно» выставляется студенту, если он допускает существенные ошибки и

			неправильно выполняет практические задания

Примерный перечень вопросов для устного опроса

1. Что такое информационная безопасность?
2. Что относится к основным принципам обеспечения безопасности?
3. Что относится к национальным интересам в информационной сфере?
4. На каких принципах основывается деятельность государственных органов по обеспечению информационной безопасности?
5. Что такое правовое обеспечение информационной безопасности?
6. Дайте определение информационным правоотношениям.
7. Перечислите основные концептуальные документы в области информационной безопасности.
8. Каково содержание Конституции Российской Федерации о правах и обязанностях граждан России в сфере обеспечения информационной безопасности?
9. Что понимается под информационной сферой как сферой правового регулирования?
10. Приведите известные Вам понятия «информация».
11. Что такое защищаемая информация и каковы ее отличительные признаки?
12. Перечислите известные Вам критерии классификации защищаемой информации.
13. К какой информации не может быть ограничен доступ?
14. Какие сведения относятся к информации с ограниченным доступом?
15. Что понимается под термином «государственная тайна»?

Примерные тесовые задания

1. 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.

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. 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.

3. 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.

4. 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.

Примерные практические задания

1. Разработать примерный перечень сведений, персональные данные, используя необходимые нормативные правовые акты.

2. Разработать примерный перечень мероприятий по обеспечению физической безопасности объекта, содержащих государственную тайну.

3. Разработать примерный перечень мероприятий по обеспечению физической безопасности объекта, содержащих конфиденциальную информацию.

4. Используя необходимые нормативные правовые документы, приведите порядок проведения сертификация и контроля средств защиты информации.

5. Используя соответствующие нормативно-правовые документы определите порядок действий по получению лицензии на деятельность, связанную с защитой государственной тайны.

6. Используя необходимые нормативные правовые документы, приведите порядок проведения сертификация и контроля средств защиты информации.

7. Сотрудник фирмы «Сибинтек» Левченко, пользуясь правами администратора сетей и имея доступ к содержащейся в АС 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.

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине

Компетенция ОПК-5 (ОПК-5.3; ОПК-5.5; ОПК-5.6; ОПК-5.7; ОПК-5.8, ОПК-5.9, ОПК-5.10, ОПК-5.11)

Вопросы с выбором

1. 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.

2. 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.

3. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в:
а) Конституции РФ;
б) Гражданском кодексе РФ;
в) Доктрине информационной безопасности РФ;
г) Федеральном законе «Об информации, информационных технологиях и о защите информации».

4. 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.

5. 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».

6. 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.

7. 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.

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. 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.

10. 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.

11. 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.

12. 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.

13. Каким нормативным правовым документом утверждены правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности?
а) Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203;
б) Указ Президента Российской Федерации от 6 марта 1997 г. № 188;
в) Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870;
г) Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

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. Какие категории персональных данных выделяет Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?
а) общедоступные персональные данные, специальные категории персональных данных, категории персональных данных, обрабатываемые в информационных системах персональных данных, биометрические персональные данные;
б) общедоступные персональные данные, специальные категории персональных данных, биометрические персональные данные и иные;
в) общедоступные персональные данные, категории персональных данных, обрабатываемые в информационных системах персональных данных;
г) данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

16. 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.

17. Соблюдение каких правил входит в защиту правомочий обладателя информации?
а) соблюдение конфиденциальности информации **–** свойство информационной технологии (ИТ) обеспечивать раскрытие информации только в соответствии с правилами разграничения доступа (право распоряжения);
б) соблюдение целостности информации **–** свойство ИТ обеспечивать предоставление права модификации (уничтожения) информации только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность информации в условиях случайных ошибок или стихийных бедствий (право владения);
в) соблюдение доступности информации **–** свойство ИТ обеспечивать свободный доступ к информации по мере возникновения необходимости (право пользования);
г) соблюдение всех перечисленных правил.

18. Какая из перечисленных видов тайн относится к категории конфиденциальной информации?
а) государственная тайна, персональные данные, коммерческая тайна, служебная тайна;
б) персональные данные, коммерческая тайна, служебная тайна;
в) государственная тайна, коммерческая тайна, служебная тайна;
г) секретные сведения, совершенно секретные сведения, сведения особой важности.

19. Каков срок засекречивания сведений, составляющих государственную тайну?
а) 10 лет;
б) 20 лет;
в) 30 лет;
г) 40 лет.

20. Как часто органы государственной власти должны пересматривать перечни сведений, подлежащих засекречиванию?
а) каждые 3 года;
б) каждые 5 лет;
в) каждые 7 лет;
г) каждые 10 лет.

21. 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.

22. Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных:
а) осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник;
б) необходима в связи с осуществлением правосудия;
в) необходима в связи с выездом за пределы Российской Федерации;
г) необходима в соответствии с оперативно-розыскной деятельностью.

23. Режим документированной информации – это:
а) электронный документ с электронной подписью;
б) выделенная информация по определенной цели;
в) выделенная информация в любой знаковой форме;
г) электронная информация, позволяющая ее идентифицировать.

24. В правовой режим документированной информации входит:
а) государственная тайна;
б) банковская тайна;
в) персональные данные;
г) электронная цифровая подпись.

25. Засекречиванию подлежат сведения о:
а) фактах нарушения прав и свобод человека и гражданина;
б) состоянии демографии;
в) силах и средствах гражданской обороны;
г) состоянии преступности.

26. 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.

27. 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.

28. К государственной тайне не относятся сведения, защищаемые государством, распространение которых может нанести ущерб государству:
а) в экономической области;
б) в контрразведывательной деятельности;
в) в оперативно-разыскной деятельности;
г) о частной жизни политических деятелей.

29. Обработка персональных данных – это:
а) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
б) накопление, хранение и передача персональных данных;
в) размещение персональных данных в информационных системах;
г) только передача персональных данных.

30. Срок хранения персональных данных, осуществляемого в форме, позволяющей определить субъекта персональных данных:
а) 1 год;
б) 5 лет;
в) Не дольше, чем этого требуют цели обработки персональных данных, если иное не установлено законом или договором;
г) 3 года.

31. 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.

32. Доктрина информационной безопасности не закрепляет следующие термины:
а) информация;
б) информационная безопасность Российской Федерации;
в) информационная угроза;
г) средства обеспечения информационной безопасности.

33. 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.

34. 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).

35. В соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн устанавливается:
а) два уровня защищенности персональных данных;
б) три уровня защищенности персональных данных;
в) четыре уровня защищенности персональных данных;
г) пять уровней защищенности персональных данных.

36. При проведении контроля за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах персональных данных регуляторы:
а) вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных;
б) не вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных;
в) вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных, только в установленных законом случаях;
г) не вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных во всех случаях.

37. В соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994) на какой орган исполнительной власти РФ возложены полномочия по аккредитации органов по аттестации объектов информатизации?
а) ФСБ России;
б) МВД России;
в) ФСО России;
г) ФСТЭК России.

38. В соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994) какие объекты информатизации подлежат обязательной аттестации?
а) предназначенные для обработки персональных данных;

б) предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров;
в) предназначенные для обработки конфиденциальной информации;
г) предназначенные для обмена информацией, составляющей государственную тайну.

39. 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.

40. Каким нормативным правовым документом утверждено Положение о Федеральной службе по техническому и экспортному контролю?
а) Приказом ФСТЭК России от 3 марта 2011 г. № 116;
б) Указом Президента Российской Федерации от 16 августа 2004 г. № 1085;
в) Федеральным законом от 18 июля 1999 г. № 183-ФЗ;
г) Постановлением Правительства Российской Федерации от 15 апреля 1995 г. № 333.

41. 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.

42. Объектами авторского права не являются:
а) программы для электронных вычислительных машин (программы для ЭВМ);
б) литературные произведения;
в) изобретения;
г) аудиовизуальные произведения.

43. Объектами патентного права не являются:
а) программы для электронных вычислительных машин (программы для ЭВМ);
б) полезные модели;
в) промышленные образцы;
г) изобретения.

44. Каким нормативным правовым документом регламентированы вопросы государственной регистрации программ для ЭВМ и баз данных?
а) Законом РФ от 23.09.1992 № 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных»;
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 закон Российской Федерации от 23.09.1992 № 3517-1.

45. 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.

46. К показателям патентоспособности изобретения относятся:
а) новизна, наличие изобретательского уровня, промышленная применимость;
б) новизна, промышленная применимость;
в) возможность многократного воспроизведения образца путем производства соответствующего изделия, новизна, наличие изобретательского уровня, промышленная применимость;
г) возможность многократного воспроизведения образца путем производства соответствующего изделия, новизна, оригинальность, промышленная применимость.

47. 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.

48. 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.

49. 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.

50. Каким нормативным правовым документом утверждены виды средств защиты информации, подлежащих сертификации в системе сертификации СЗИ-ГТ?
а) Приказом Гостехкомиссии РФ от 27.10.1995 № 199;
б*) Приказом ФСБ РФ от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;*
в) Постановлением Правительства РФ от 01.12.2009 № 982;
г) Приказом ФСТЭК России от 11.02.2013 № 17.

51. 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.

52. 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.

53. Какой вид ответственности предусмотрен действующим законодательством в случае занятия видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии?
а) уголовная ответственность;
б) административная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

54. 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.

55. 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.

56. 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.

57. 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.

58. 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.

59. Какой вид ответственности предусмотрен действующим законодательством в случае получения сведений, составляющих государственную тайну, путем похищения, обмана, шантажа, принуждения, угрозы применения насилия либо иным незаконным способом?
а) уголовная ответственность;
б) административная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

60. 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.

Вопросы с коротким ответом

61. Верно ли утверждение «информация - сведения (сообщения, данные) независимо от формы их представления»?

62. Каким нормативным правовым документом определен термин «Информационная безопасность Российской Федерации»?

63. Может ли быть ограничен доступ к информации о состоянии окружающей среды (экологической информации)?

64. К какому виду защищаемых сведений относятся сведения, составляющие тайну следствия и судопроизводства?

65. Каким нормативным правовым документом определен перечень сведений, не подлежащих отнесению к государственной тайне и засекречиванию?

66. Является ли основанием для отказа должностному лицу или гражданину в допуске к государственной тайне постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства?

67. Должно ли уведомление об обработке персональных данных содержать дату начала обработки персональных данных, а также срок или условие прекращения обработки персональных данных?

68. Какой федеральный орган исполнительной власти является Уполномоченным органом по защите прав субъектов персональных данных?

69. Какая пометка проставляется на документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения?

70. Каков срок засекречивания сведений, составляющих государственную тайну?

71. Сколько типов актуальных угроз безопасности персональных данных определено Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»?

72. Сколько уровней защищенности персональных данных при их обработке в информационных системах установлено действующими нормативными правовыми документами?

73. Какой нормативный правовой акт, регулирующий информационные отношения является базовым?

74. Верно ли утверждение «коммерческая тайна - 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»

75. Составляют ли сведения о задолженности работодателей по выплате заработной платы и социальным выплатам коммерческую тайну?

Вопросы с развернутым ответом

76. Что такое защита информации в соответствии с «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введенным в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст)?

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение защиты информации.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение защиты информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение защиты информации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение защиты информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

77. Что такое технический канал утечки информации в соответствии с «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введенным в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст):

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение технического канала утечки информации.	Отлично (90-100 баллов)

Обучающийся приводит полное и безошибочное определение технического канала утечки информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение технического канала утечки информации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение технического канала утечки информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

78. Что понимается под несанкционированным доступом (НСД) к информации в соответствии с «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введенным в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст):

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение несанкционированного доступа (НСД) к информации.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение несанкционированного доступа (НСД) к информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение несанкционированного доступа (НСД) к информации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение несанкционированного доступа (НСД) к информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

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

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение угрозы безопасности информации.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение угроза безопасности информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение угроза безопасности информации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение угроза безопасности информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

80. Раскройте сущность понятия специальное исследование (объекта защиты информации).

Критерии оценивания	Шкала оценок

Обучающийся приводит полное и безошибочное раскрытие сущности понятия специальные исследования.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное раскрытие сущности понятия специальные исследования. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное раскрытие сущности понятия специальные исследования.	Удовлетворительно (50-70 баллов)
Представлено неполное раскрытие сущности понятия специальные исследования. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

81. Раскройте сущность понятия Специальная проверка.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное раскрытие сущности понятия специальная проверка.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное раскрытие сущности понятия специальная проверка. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное раскрытие сущности понятия специальная проверка.	Удовлетворительно (50-70 баллов)
Представлено неполное раскрытие сущности понятия специальная проверка. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

82. Что понимается под термином «объект информатизации»?

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение термина объект информатизации.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение термина объект информатизации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение термина объект информатизации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение термина объект информатизации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

83. Что понимается под угрозой безопасности персональных данных в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»?

Критерии оценивания	Шкала оценок

Обучающийся приводит полное и безошибочное определение угрозы безопасности персональных данных.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение угрозы безопасности персональных данных. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение угрозы безопасности персональных данных.	Удовлетворительно (50-70 баллов)
Представлено неполное определение угрозы безопасности персональных данных. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

84. 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» какие органы, уполномочены на ведение лицензионной деятельности на право проведения работ, связанных с созданием средств защиты информации?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень федеральных органов исполнительной власти.	Отлично (90-100 баллов)
Обучающийся приводит полный и безошибочный перечень федеральных органов исполнительной власти. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлен неполный перечень федеральных органов исполнительной власти.	Удовлетворительно (50-70 баллов)
Представлен неполный перечень федеральных органов исполнительной власти. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

85. Что означает термин «лицензиат»?

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение термина лицензиат.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение термина лицензиат. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение термина лицензиат.	Удовлетворительно (50-70 баллов)
Представлено неполное определение термина лицензиат. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

86. Что такое политика безопасности (информации в организации) в соответствии с «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введенным в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст?

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение термина политика безопасности (информации в организации).	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение термина политика безопасности (информации в организации). Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение термина политика безопасности (информации в организации).	Удовлетворительно (50-70 баллов)
Представлено неполное определение термина политика безопасности (информации в организации). Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

87. Раскройте сущность понятия «экспертиза документа по защите информации» в соответствии с действующими руководящими документами.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное раскрытие сущности понятия «экспертиза документа по защите информации».	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное раскрытие сущности понятия «экспертиза документа по защите информации». Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное раскрытие сущности понятия «экспертиза документа по защите информации».	Удовлетворительно (50-70 баллов)
Представлено неполное раскрытие сущности понятия «экспертиза документа по защите информации». Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

88. Что относится к общедоступным персональным данным в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень сведений, относящихся к общедоступным персональным данным со ссылкой на номер статьи ФЗ-152 «О персональных данных»	Отлично (90-100 баллов)

Обучающийся приводит полный и безошибочный перечень сведений, относящихся к общедоступным персональным данным. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлен неполный перечень сведений, относящихся к общедоступным персональным данным.	Удовлетворительно (50-70 баллов)
Представлен неполный перечень сведений, относящихся к общедоступным персональным данным. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

89. В соответствии с какими принципами осуществляется отнесение сведений к государственной тайне и их засекречивание в соответствии с Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне»? Раскройте их сущность.

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень принципов отнесения сведений к государственной тайне и их засекречивания, раскрывает их сущность.	Отлично (90-100 баллов)
Обучающийся приводит полный и безошибочный перечень сведений, относящихся к общедоступным персональным данным. Допускаются незначительные неточности а раскрытии их сущности	Хорошо (70-80 баллов)
Представлен неполный перечень принципов отнесения сведений к государственной тайне и их засекречивания, сущность их раскрыта неполно.	Удовлетворительно (50-70 баллов)
Представлен неполный перечень принципов отнесения сведений к государственной тайне и их засекречивания, сущность их не раскрыта. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

90. Какие степени секретности сведений, составляющих государственную тайну установлены действующим законодательством?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень степеней секретности сведений, составляющих государственную тайну. Называет нормативный правовой акт, устанавливающий данные степени.	Отлично (90-100 баллов)
Обучающийся приводит полный и безошибочный перечень степеней секретности сведений, составляющих государственную тайну. Называет нормативный правовой акт, устанавливающий данные степени. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлен полный перечень степеней секретности сведений, составляющих государственную	Удовлетворительно (50-70 баллов)

тайну. Не называет нормативный правовой акт, устанавливающий данные степени.	
Представлен неполный перечень степеней секретности сведений, составляющих государственную тайну. Не называет нормативный правовой акт, устанавливающий данные степени. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

Компетенция ОПК-6 (ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6, ОПК- 6.7, ОПК-6.8, ОПК-6.9, ОПК-6.10)

Вопросы с выбором

1. 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.

2. 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.

3. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в:

а) Конституции РФ;

б) Гражданском кодексе РФ;

в) Доктрине информационной безопасности РФ;

г) Федеральном законе «Об информации, информационных технологиях и о защите информации».

4. 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.

5. 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».

6. 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.

7. 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.

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. 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.

10. 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.

11. 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.

12. 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.

13. Каким нормативным правовым документом утверждены правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности?
а) Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203;
б) Указ Президента Российской Федерации от 6 марта 1997 г. № 188;
в) Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870;
г) Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

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. Какие категории персональных данных выделяет Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?
а) общедоступные персональные данные, специальные категории персональных данных, категории персональных данных, обрабатываемые в информационных системах персональных данных, биометрические персональные данные;
б) общедоступные персональные данные, специальные категории персональных данных, биометрические персональные данные и иные;
в) общедоступные персональные данные, категории персональных данных, обрабатываемые в информационных системах персональных данных;
г) данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

16. 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.

17. Соблюдение каких правил входит в защиту правомочий обладателя информации?
а) соблюдение конфиденциальности информации **–** свойство информационной технологии (ИТ) обеспечивать раскрытие информации только в соответствии с правилами разграничения доступа (право распоряжения);
б) соблюдение целостности информации **–** свойство ИТ обеспечивать предоставление права модификации (уничтожения) информации только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность информации в условиях случайных ошибок или стихийных бедствий (право владения);
в) соблюдение доступности информации **–** свойство ИТ обеспечивать свободный доступ к информации по мере возникновения необходимости (право пользования);
г) соблюдение всех перечисленных правил.

18. Какая из перечисленных видов тайн относится к категории конфиденциальной информации?

а) государственная тайна, персональные данные, коммерческая тайна, служебная тайна;
б) персональные данные, коммерческая тайна, служебная тайна;
в) государственная тайна, коммерческая тайна, служебная тайна;
г) секретные сведения, совершенно секретные сведения, сведения особой важности.

19. Каков срок засекречивания сведений, составляющих государственную тайну?
а) 10 лет;
б) 20 лет;
в) 30 лет;
г) 40 лет.

20. Как часто органы государственной власти должны пересматривать перечни сведений, подлежащих засекречиванию?
а) каждые 3 года;
б) каждые 5 лет;
в) каждые 7 лет;
г) каждые 10 лет.

21. 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.

22. Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных:
а) осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник;
б) необходима в связи с осуществлением правосудия;
в) необходима в связи с выездом за пределы Российской Федерации;
г) необходима в соответствии с оперативно-розыскной деятельностью.

23. Режим документированной информации – это:
а) электронный документ с электронной подписью;
б) выделенная информация по определенной цели;
в) выделенная информация в любой знаковой форме;
г) электронная информация, позволяющая ее идентифицировать.

24. В правовой режим документированной информации входит:
а) государственная тайна;
б) банковская тайна;
в) персональные данные;
г) электронная цифровая подпись.

25. Засекречиванию подлежат сведения о:
а) фактах нарушения прав и свобод человека и гражданина;
б) состоянии демографии;
в) силах и средствах гражданской обороны;
г) состоянии преступности.

26. 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.

27. 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.

28. К государственной тайне не относятся сведения, защищаемые государством, распространение которых может нанести ущерб государству:
а) в экономической области;
б) в контрразведывательной деятельности;
в) в оперативно-разыскной деятельности;
г) о частной жизни политических деятелей.

29. Обработка персональных данных – это:
а) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
б) накопление, хранение и передача персональных данных;
в) размещение персональных данных в информационных системах;
г) только передача персональных данных.

30. Срок хранения персональных данных, осуществляемого в форме, позволяющей определить субъекта персональных данных:
а) 1 год;
б) 5 лет;
в) Не дольше, чем этого требуют цели обработки персональных данных, если иное не установлено законом или договором;
г) 3 года.

31. 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.

32. Доктрина информационной безопасности не закрепляет следующие термины:
а) информация;
б) информационная безопасность Российской Федерации;
в) информационная угроза;
г) средства обеспечения информационной безопасности.

33. 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.

34. 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).

35. В соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн устанавливается:
а) два уровня защищенности персональных данных;
б) три уровня защищенности персональных данных;
в) четыре уровня защищенности персональных данных;
г) пять уровней защищенности персональных данных.

36. При проведении контроля за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах персональных данных регуляторы:
а) вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных;
б) не вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных;
в) вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных, только в установленных законом случаях;
г) не вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных во всех случаях.

37. В соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994) на какой орган исполнительной власти РФ возложены полномочия по аккредитации органов по аттестации объектов информатизации?
а) ФСБ России;
б) МВД России;
в) ФСО России;
г) ФСТЭК России.

38. В соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994) какие объекты информатизации подлежат обязательной аттестации?
а) предназначенные для обработки персональных данных;
б) предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров;
в) предназначенные для обработки конфиденциальной информации;
г) предназначенные для обмена информацией, составляющей государственную тайну.

39. 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.

40. Каким нормативным правовым документом утверждено Положение о Федеральной службе по техническому и экспортному контролю?
а) Приказом ФСТЭК России от 3 марта 2011 г. № 116;
б) Указом Президента Российской Федерации от 16 августа 2004 г. № 1085;
в) Федеральным законом от 18 июля 1999 г. № 183-ФЗ;
г) Постановлением Правительства Российской Федерации от 15 апреля 1995 г. № 333.

41. 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.

42. Объектами авторского права не являются:
а) программы для электронных вычислительных машин (программы для ЭВМ);
б) литературные произведения;
в) изобретения;
г) аудиовизуальные произведения.

43. Объектами патентного права не являются:
а) программы для электронных вычислительных машин (программы для ЭВМ);
б) полезные модели;
в) промышленные образцы;
г) изобретения.

44. Каким нормативным правовым документом регламентированы вопросы государственной регистрации программ для ЭВМ и баз данных?
а) Законом РФ от 23.09.1992 № 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных»;
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 закон Российской Федерации от 23.09.1992 № 3517-1.

45. 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.

46. К показателям патентоспособности изобретения относятся:
а) новизна, наличие изобретательского уровня, промышленная применимость;
б) новизна, промышленная применимость;
в) возможность многократного воспроизведения образца путем производства соответствующего изделия, новизна, наличие изобретательского уровня, промышленная применимость;
г) возможность многократного воспроизведения образца путем производства соответствующего изделия, новизна, оригинальность, промышленная применимость.

47. 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.

48. 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.

49. 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.

50. Каким нормативным правовым документом утверждены виды средств защиты информации, подлежащих сертификации в системе сертификации СЗИ-ГТ?
а) Приказом Гостехкомиссии РФ от 27.10.1995 № 199;

б*) Приказом ФСБ РФ от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;*
в) Постановлением Правительства РФ от 01.12.2009 № 982;
г) Приказом ФСТЭК России от 11.02.2013 № 17.

51. 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.

52. 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.

53. Какой вид ответственности предусмотрен действующим законодательством в случае занятия видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии?
а) уголовная ответственность;
б) административная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

54. 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.

55. 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.

56. 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.

57. 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.

58. 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.

59. Какой вид ответственности предусмотрен действующим законодательством в случае получения сведений, составляющих государственную тайну, путем похищения, обмана, шантажа, принуждения, угрозы применения насилия либо иным незаконным способом?
а) уголовная ответственность;
б) административная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

60. 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.

Вопросы с коротким ответом

61. Верно ли утверждение «информация - сведения (сообщения, данные) независимо от формы их представления»?

62. Каким нормативным правовым документом определен термин «Информационная безопасность Российской Федерации»?

63. Может ли быть ограничен доступ к информации о состоянии окружающей среды (экологической информации)?

64. К какому виду защищаемых сведений относятся сведения, составляющие тайну следствия и судопроизводства?

65. Каким нормативным правовым документом определен перечень сведений, не подлежащих отнесению к государственной тайне и засекречиванию?

66. Является ли основанием для отказа должностному лицу или гражданину в допуске к государственной тайне постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства?

67. Должно ли уведомление об обработке персональных данных содержать дату начала обработки персональных данных, а также срок или условие прекращения обработки персональных данных?

68. Какой федеральный орган исполнительной власти является Уполномоченным органом по защите прав субъектов персональных данных?

69. Какая пометка проставляется на документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения?

70. Каков срок засекречивания сведений, составляющих государственную тайну?

71. Сколько типов актуальных угроз безопасности персональных данных определено Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»?

72. Сколько уровней защищенности персональных данных при их обработке в информационных системах установлено действующими нормативными правовыми документами?

73. Какой нормативный правовой акт, регулирующий информационные отношения является базовым?

74. Верно ли утверждение «коммерческая тайна - 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»

75. Составляют ли сведения о задолженности работодателей по выплате заработной платы и социальным выплатам коммерческую тайну?

Вопросы с развернутым ответом

76. Что такое защита информации в соответствии с «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введенным в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст)?

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение защиты информации.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение защиты информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение защиты информации.	Удовлетворительно (50-70 баллов)

Представлено неполное определение защиты информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

77. Что такое технический канал утечки информации в соответствии с «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введенным в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст):

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение технического канала утечки информации.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение технического канала утечки информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение технического канала утечки информации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение технического канала утечки информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

78. Что понимается под несанкционированным доступом (НСД) к информации в соответствии с «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введенным в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст):

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение несанкционированного доступа (НСД) к информации.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение несанкционированного доступа (НСД) к информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение несанкционированного доступа (НСД) к информации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение несанкционированного доступа (НСД) к информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

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

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение угрозы безопасности информации.	Отлично (90-100 баллов)

Обучающийся приводит полное и безошибочное определение угроза безопасности информации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение угроза безопасности информации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение угроза безопасности информации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

80. Раскройте сущность понятия специальное исследование (объекта защиты информации).

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное раскрытие сущности понятия специальные исследования.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное раскрытие сущности понятия специальные исследования. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное раскрытие сущности понятия специальные исследования.	Удовлетворительно (50-70 баллов)
Представлено неполное раскрытие сущности понятия специальные исследования. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

81. Раскройте сущность понятия Специальная проверка.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное раскрытие сущности понятия специальная проверка.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное раскрытие сущности понятия специальная проверка. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное раскрытие сущности понятия специальная проверка.	Удовлетворительно (50-70 баллов)
Представлено неполное раскрытие сущности понятия специальная проверка. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

82. Что понимается под термином «объект информатизации»?

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение термина объект информатизации.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение термина объект информатизации. Допускаются незначительные неточности.	Хорошо (70-80 баллов)

Представлено неполное определение термина объект информатизации.	Удовлетворительно (50-70 баллов)
Представлено неполное определение термина объект информатизации. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

83. Что понимается под угрозой безопасности персональных данных в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»?

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение угрозы безопасности персональных данных.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение угрозы безопасности персональных данных. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение угрозы безопасности персональных данных.	Удовлетворительно (50-70 баллов)
Представлено неполное определение угрозы безопасности персональных данных. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

84. 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» какие органы, уполномочены на ведение лицензионной деятельности на право проведения работ, связанных с созданием средств защиты информации?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень федеральных органов исполнительной власти.	Отлично (90-100 баллов)
Обучающийся приводит полный и безошибочный перечень федеральных органов исполнительной власти. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлен неполный перечень федеральных органов исполнительной власти.	Удовлетворительно (50-70 баллов)
Представлен неполный перечень федеральных органов исполнительной власти. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

85. Что означает термин «лицензиат»?

Критерии оценивания	Шкала оценок

Обучающийся приводит полное и безошибочное определение термина лицензиат.	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение термина лицензиат. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение термина лицензиат.	Удовлетворительно (50-70 баллов)
Представлено неполное определение термина лицензиат. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

86. Что такое политика безопасности (информации в организации) в соответствии с «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введенным в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст?

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение термина политика безопасности (информации в организации).	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное определение термина политика безопасности (информации в организации). Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное определение термина политика безопасности (информации в организации).	Удовлетворительно (50-70 баллов)
Представлено неполное определение термина политика безопасности (информации в организации). Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

87. Раскройте сущность понятия «экспертиза документа по защите информации» в соответствии с действующими руководящими документами.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное раскрытие сущности понятия «экспертиза документа по защите информации».	Отлично (90-100 баллов)
Обучающийся приводит полное и безошибочное раскрытие сущности понятия «экспертиза документа по защите информации». Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено неполное раскрытие сущности понятия «экспертиза документа по защите информации».	Удовлетворительно (50-70 баллов)
Представлено неполное раскрытие сущности понятия «экспертиза документа по защите информации». Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

88. Что относится к общедоступным персональным данным в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень сведений, относящихся к общедоступным персональным данным со ссылкой на номер статьи ФЗ-152 «О персональных данных»	Отлично (90-100 баллов)
Обучающийся приводит полный и безошибочный перечень сведений, относящихся к общедоступным персональным данным. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлен неполный перечень сведений, относящихся к общедоступным персональным данным.	Удовлетворительно (50-70 баллов)
Представлен неполный перечень сведений, относящихся к общедоступным персональным данным. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

89. В соответствии с какими принципами осуществляется отнесение сведений к государственной тайне и их засекречивание в соответствии с Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне»? Раскройте их сущность.

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень принципов отнесения сведений к государственной тайне и их засекречивания, раскрывает их сущность.	Отлично (90-100 баллов)
Обучающийся приводит полный и безошибочный перечень сведений, относящихся к общедоступным персональным данным. Допускаются незначительные неточности а раскрытии их сущности	Хорошо (70-80 баллов)
Представлен неполный перечень принципов отнесения сведений к государственной тайне и их засекречивания, сущность их раскрыта неполно.	Удовлетворительно (50-70 баллов)
Представлен неполный перечень принципов отнесения сведений к государственной тайне и их засекречивания, сущность их не раскрыта. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

90. Какие степени секретности сведений, составляющих государственную тайну установлены действующим законодательством?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень степеней секретности сведений, составляющих государственную тайну. Называет нормативный правовой акт, устанавливающий данные степени.	Отлично (90-100 баллов)

Обучающийся приводит полный и безошибочный перечень степеней секретности сведений, составляющих государственную тайну. Называет нормативный правовой акт, устанавливающий данные степени. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлен полный перечень степеней секретности сведений, составляющих государственную тайну. Не называет нормативный правовой акт, устанавливающий данные степени.	Удовлетворительно (50-70 баллов)
Представлен неполный перечень степеней секретности сведений, составляющих государственную тайну. Не называет нормативный правовой акт, устанавливающий данные степени. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

20.2. Промежуточная аттестация

Примерный перечень вопросов к зачету с оценкой

№	Содержание
1	Место информационной безопасности в системе национальной безопасности РФ.
2	Понятие и сущность защиты информации
3	Понятие и содержание правового обеспечения информационной безопасности
4	Понятие и содержание организационного обеспечения информационной безопасности
5	Безопасность государства: содержание и принципы обеспечения
6	Стратегия национальной безопасности РФ
7	Информация и информационные системы – объекты правоотношений в сфере обеспечения информационной безопасности.
8	Конституционные гарантии прав граждан на информацию.
9	Конституция РФ о правах и обязанностях граждан России в сфере обеспечения информационной безопасности.
10	Место физической безопасности в обеспечении комплексной защиты информации.
11	Понятие и сущность государственной тайны
12	Административная ответственность за нарушения правовых норм в сфере защиты информации.
13	Виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
14	Международное законодательство в области защиты информации.
15	Защита интеллектуальной собственности в системе правового регулирования информационной безопасности.
16	Механизм ограничения доступа к сведениям, составляющим государственную тайну.
17	Организационные аспекты получения лицензии на занятие определенным видом деятельности в сфере обеспечения информационной безопасности.
18	Организационные аспекты получения сертификата соответствия на средства защиты информации.
19	Направления государственной политики РФ в сфере обеспечения информационной безопасности.
20	Организационная структура системы государственного лицензирования.
21	Организационно-правовая система обеспечения защиты объектов промышленной собственности на основе патентов.
22	Классификация и структура нормативных правовых актов в сфере обеспечения защиты информации.
23	Организационная основа системы информационной безопасности РФ.
24	Организация пропускного и внутриобъектового режимов.

25	Основные положения патентного права.
26	Основные положения по защите служебной тайны.
27	Основные положения Федерального закона от 27 декабря 2002г. №184-ФЗ «О техническом регулировании».
28	Основные положения Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
29	Основные понятия и положения системы государственного лицензирования.
30	Основные понятия и система сертификации продукции и услуг.
31	Особенности юридической ответственности за нарушения норм защиты информации в области трудовых и гражданско-правовых отношений.
32	Ответственность в сере защиты государственной тайны.
33	Ответственность за правонарушения в сфере лицензирования и сертификации.
34	Понятие и виды защищаемой информации.
35	Понятие и задачи государственной системы обеспечения информационной безопасности в РФ.
36	Основные меры по обеспечению сохранности носителей конфиденциальной
37	Основные положения Доктрины информационной безопасности Российской Федерации.
38	Понятие и классификация видов правонарушений в сфере защиты информации
39	Понятие и содержание национальных интересов Российской Федерации в информационной сфере в соответствии с Доктриной информационной безопасности
40	Основные принципы организации и проведения комплексных специальных проверок.
41	Угрозы информационной безопасности личности, обществу и государству.
42	Формы организационной защиты информации.
43	Структура государственной системы информационной безопасности в РФ.
44	Структура государственной системы правового регулирования информационной безопасности в РФ.
45	Основы авторского права.
46	Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
47	Основы противодействия противоправных действий в сфере защиты информации.
48	Особенности правовой охраны программ для ЭВМ и баз данных.
49	Особенности правовой охраны топологий интегральных микросхем. Понятие комплексной защиты информации на объекте.
50	Понятие юридической ответственности за нарушение правовых норм в области информационной безопасности.
51	Особенности сертификации средств защиты информации.
52	Понятие и содержание правового обеспечения информационной безопасности
53	Методы организационной защиты информации.
54	Классификация помещений в зависимости от условий доступа.
55	Основные положения аттестации объектов информатизации по требованиям безопасности информации.
56	Правовая основа обеспечения защиты государственной тайны.
57	Правовая основа обеспечения защиты коммерческой тайны.
58	Правовая основа обеспечения защиты персональных данных.
59	Правовая основа обеспечения защиты служебной тайны.
60	Правовое регулирование защиты сведений, связанных с профессиональной деятельностью
61	Содержание методов обеспечения физической безопасности.
62	Функции элементов организационной основы системы информационной безопасности РФ.
63	Характеристика угроз информационной безопасности в соответствии с Доктриной информационной безопасности.
64	Уголовная ответственность за нарушение правовых норм в сфере защиты информации.

65	Уголовная ответственность за нарушение правовых норм, предусмотренных главой 28 УК РФ.
66	Направления деятельности ФСТЭК России в сфере обеспечения информационной безопасности.
67	Деятельность контрольно-надзорных органов в сфере обеспечения безопасности персональных данных.
68	Направления деятельности ФСБ России в сфере обеспечения информационной безопасности.

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
«____»_____ 2023

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.О.49 Организационное и правовое обеспечение информационной безопасности
Форма обучения Очное

Вид контроля зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Ответственность за правонарушения в сфере лицензирования и сертификации.
2. Персональные данные как вид защищаемой информации: понятие, правовое регулирование, виды персональных данных.

Практическое задание: разработайте план организационных мероприятий по защите объекта информатизации.

Преподаватель _____ Н.В. Филиппова

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше.