

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



10.06.2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.40 Организационное и правовое обеспечение информационной безопасности

1. Код и наименование направления подготовки/специальности:

10.03.01 Информационная безопасность

2. Профиль подготовки/специализация: Безопасность компьютерных систем

3. Квалификация выпускника: Бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации ФКН

6. Составители программы:

Филиппова Неля Викторовна, к.ю.н, доцент

7. Рекомендована: протокол НМС ФКН № 5 от 25.04.2022 г

8. Учебный год: 2023-2024

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 относится 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 в сфере профессиональной деятельности;	ОПК-5.1	знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;	Знать: основы правового обеспечения информационной безопасности; основные положения законодательства РФ в области информационной безопасности права, свободы и обязанности личности в области информационной безопасности; 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-	Способен	ОПК-5.2	знает основные	Знать: основные категории, понятия,

5	применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;		понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации;	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 в сфере профессиональной деятельности;	ОПК-5.3	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 в сфере профессиональной деятельности;	ОПК-5.4	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 актов 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	ОПК-5.5	умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных	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

	документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;		обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;	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 в сфере профессиональной деятельности;	ОПК-5.6	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 в сфере профессиональной деятельности;	ОПК-5.7	умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;	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 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	ОПК-5.8	умеет формулировать основные требования по защите конфиденциальной информации,	Уметь: формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации на основе

	методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;		персональных данных и охране результатов интеллектуальной деятельности в организации;	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 соответствии с нормативными правовыми актами, нормативными и 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	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 соответствии с нормативными правовыми актами, нормативными и 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	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;

	защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;			Уметь: применять организационные меры защиты информации ограниченного доступа;
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.4	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 соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.5	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

	Федерации, Федеральной службы по техническому и экспортному контролю;			
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.6	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

12. Объем дисциплины в зачетных единицах/час. — 3/108.

Форма промежуточной аттестации: экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра - 4	№ семестра	итого
Аудиторные занятия	50	50		50
в том числе:	лекции	16	16	16
	практические	34	34	34
	лабораторные			
Самостоятельная работа	22	22		22
в том числе: курсовая работа (проект)				
Форма промежуточной аттестации (экзамен – 36 час.)	36	36		36
Итого:	108	108		108

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	Место информационной безопасности в системе национальной безопасности РФ. Понятие, структура и содержание информационной безопасности. Угрозы информационной	

	безопасности РФ. Законодательство в области обеспечения информационной безопасности	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	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-	

	информационной безопасности	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 тайна 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 защиты 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)				Всего
		Лекции	Практические	Лабораторные	Самостоятельная работа	
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	2	6		4	12

	информатизации				
	Итого:	16	34	22	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	<i>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.</i>
2	<i>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.</i>

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	«Университетская библиотека online» - контракт №3010-06/30-21 от 23.12.2021
2	«Консультант студента» - контракт №3010-06/29-21 от 23.12.2021

3	ЭБС «Лань» - контракт №3010-06/01-22 от 10.03.2022; лицензионный договор №3010-06/02-22 от 10.03.2022; лицензионный договор №3010-15/231-22 от 17.05.2022
4	ЭБС «Образовательная платформа ЮРАЙТ» - договор №4990 от 10.01.2022; лицензионный договор №3010-15/217-22 от 05.05.2022
5	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
6	Образовательный портал «Электронный университет ВГУ». – (https://edu.vsu.ru/)
7	Справочно-информационная система «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru .

16. Перечень учебно-методического обеспечения для самостоятельной работы

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

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 16, 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

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-5.1, ОПК-5.2, ОПК-5.5	Устный опрос Тест № 1 Практическое задание
2.	Информация как объект правового регулирования	ОПК-5	ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4, ОПК-5.5, ОПК-5.6, ОПК-5.8	Устный опрос Тест № 2 Практическое задание
3.	Правовое регулирование информационной безопасности в сфере интеллектуальной собственности	ОПК-5	ОПК-5.1, ОПК-5.2, ОПК-5.4, ОПК-5.8	Устный опрос Тест № 3 Практическое задание
4.	Правонарушения в сфере защиты информации	ОПК-5	ОПК-5.1, ОПК-5.2, ОПК-5.3	Устный опрос Тест № 4 Практическое задание
5.	Государственная система обеспечения информационной безопасности	ОПК-5 ОПК-6	ОПК-5.1, ОПК-5.5, ОПК-5.6, ОПК-6.2, ОПК-6.3, ОПК-6.6	Устный опрос Тест № 5 Практическое задание
6.	Системы лицензирования и сертификации в области защиты информации	ОПК-5 ОПК-6	ОПК-5.1, ОПК-5.3, ОПК-5.5, ОПК-5.6, ОПК-5.7, ОПК-6.1	Устный опрос Тест № 6 Практическое задание
7.	Аттестация объектов информатизации по требованиям безопасности информации	ОПК-5 ОПК-6	ОПК-5.5, ОПК-5.6, ОПК-5.7, ОПК-6.1, ОПК-6.3, ОПК-6.4, ОПК-6.5, ОПК-6.6	Устный опрос Тест № 7 Практическое задание
8.	Организационно-техническое обеспечение защиты информации на объектах информатизации	ОПК-5 ОПК-6	ОПК-5.5, ОПК-5.6, ОПК-6.1, ОПК-6.2, ОПК-6.3, ОПК-6.4, ОПК-6.5, ОПК-6.6	Устный опрос Тест № 8 Практическое задание
Промежуточная аттестация форма контроля – экзамен				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 экзамене

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

			<p>задания, не допускает существенных неточностей;</p> <p>Оценка «удовлетворительно» выставляется студенту, если он допускает неточности в ответе, испытывает затруднения в выполнении практических заданий, при указании на существенные ошибки может их исправить;</p> <p>Оценка «неудовлетворительно» выставляется студенту, если он допускает существенные ошибки и неправильно выполняет практические задания</p>
--	--	--	--

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 тестовые 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.

20.2. Промежуточная аттестация

Примерный перечень вопросов к экзамену

№	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 сфере 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 10.03.01 Информационная безопасность

Дисциплина Б1.О.40 Организационное и правовое обеспечение информационной безопасности
Форма обучения Очное

Вид контроля экзамен

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.