ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.06 ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Профиль подготовки (специализация) 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

1. Цели освоения дисциплины

совершенствование знаний, умений и навыков обучающихся, а также получение ими дополнительных знаний, умений и навыков по вопросам организационного и правового обеспечения информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.06 Организационное и правовое обеспечение информационной безопасности относится к обязательной части учебного плана. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Организационное и правовое обеспечение информационной безопасности» является основополагающей, представлен в таблице 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ОПК-2	Защита конфиденциального делопроизводства Основы управленческой деятельности Информатика Производственная технологическая практика
ОПК-5	Теория информации Производственная технологическая практика Производственная эксплуатационная практика

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ОПК-2	Основы управления информационной безопасностью Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ОПК-5	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине (модулю)**

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1 Проводит анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных инсточников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	*Знать:* возможных источники информационных угроз, цели, пути реализации и виды ущерба *Уметь:* проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба *Владеть:* методикой определения актуальных угроз
	ОПК-2.2 Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям	*Знать:* меры и мероприятия по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям *Уметь:* работать с нормативно-методической базой, в которой отображены меры и мероприятия по повышению устойчивости объектов защиты к деструктивным воздействиям *Владеть:* методами по оптимизации структуры и функциональных процессов объекта защиты

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.3 Разрабатывает, внедряет и сопровождает комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	*Знать:* комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности *Уметь:* использовать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности *Владеть:* методами обеспечения безопасности объекта защиты
	ОПК-2.4 Проводит аудит защищенности объекта информатизации в соответствии с нормативными документами	*Знать:* Нормативно-методические документы и стандарты в области проведения аудита информационной безопасности *Уметь:* проводить аудит защищенности объекта информатизации в соответствии с нормативными документами *Владеть:* Методами проведения аудита защищенности объектов информатизации
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.1 Применяет математические модели и решать задачи помехоустойчивого кодирования при проектировании защищенных автоматизированных систем	*Знать:* математические модели при проектировании защищенных автоматизированных систем *Уметь:* использовать математические модели и решать задачи при проектировании защищенных автоматизированных систем *Владеть:* Методами проектирования защищенных автоматизированных систем

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.2 Применяет технологии защиты информации при создании защищенных автоматизированных систем	*Знать:* технологии защиты информации при создании защищенных автоматизированных систем *Уметь:* применять нормативно-методическую базу при построении защиты информации при создании защищенных автоматизированных систем *Владеть:* владеть технологиями защиты информации при создании защищенных автоматизированных систем
	ОПК-5.3 Осуществляет эксплуатацию и проводить техническое обслуживание защищенных автоматизированных систем	*Знать:* нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по эксплуатации и техническому обслуживанию защищенных автоматизированных систем *Уметь:* применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по эксплуатации и техническому обслуживанию защищенных автоматизированных систем *Владеть:* нормативными правовыми актами, нормативными и методическими документами при эксплуатации и обслуживании защищенных автоматизированных систем

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.4 Проводит мониторинг функционирования защищенных автоматизированных систем	*Знать:* нормативные правовые акты, нормативные и методические документы, регламентирующие мониторинг функционирования защищенных автоматизированных систем *Уметь:* применять нормативные правовые акты, нормативные и методические документы, регламентирующие мониторинг функционирования защищенных автоматизированных систем *Владеть:* методами мониторинга функционирования защищенных автоматизированных систем

4. Объем дисциплины

Объем дисциплины Б1.О.06 Организационное и правовое обеспечение информационной безопасности составляет 5 зачетных(ые) единиц(ы) (ЗЕ), (180 академических часов), распределение объёма дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

Вид учебной работы	Итого КР	Итого СР	Семестр №6		Семестр №7	
			КР	СР	КР	СР
Лекции (Л)	34		18		16	
Лабораторные работы (ЛР)						
Практические занятия (ПЗ)	52		18		34	
Семинары(С)						
Курсовое проектирование (КП)						
Самостоятельная работа		88		34		54
Промежуточная аттестация	6		2		4	
Наименование вида промежуточной аттестации	x	x	Зачёт		Экзамен	
Всего	92	88	38	34	54	54

5. Структура и содержание дисциплины

Структура и содержание дисциплины представлены в таблице 5.1.

Таблица 5.1 – Структура и содержание дисциплины

Наименование тем	Семестр	Объем работы по видам учебных занятий, академические часы									Коды формируемых компетенций, код индикатора достижения компетенции
		лекции	Лабораторная работа	Практические занятия	семинары	Курсовое проектирование	индивидуальные домашние задания (контрольные работы)	Самостоятельное изучение вопросов	подготовка к занятиям	Промежуточная аттестация	
Тема 1. Понятие, структура информационного правоотношения. Стратегия национальной безопасности Российской Федерации. Обеспечение национальной безопасности Российской Федерации. Концепция национальной безопасности Российской Федерации. Стратегии развития информационного общества в Российской Федерации.	6	2		2					2		ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4
Раздел 2. Государственная система правового обеспечения защиты информации в Российской Федерации	6	2		2							

Тема 2. Общая характеристика информационно-правовых норм. Органы законодательства, регламентирующие деятельность по информационной безопасности. Структура органов власти по защите информации в Российской Федерации. Совет Безопасности Российской. Федерации. Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации. Федеральная служба безопасности Российской Федерации (ФСБ). Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ). Комитет по вопросам информационной безопасности. Понятие и виды защищаемой информации по российскому законодательству. Информация как объект гражданских прав.	6	2		2					4		ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4
Раздел 3. Защита персональных данных	6	6		6							

Тема 3. Регуляторы в области защиты ПДн. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных	6	6		6			20				ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4

при их обработке в информационных системах персональных данных с использованием средств автоматизации.											
Раздел 4. Режим защиты государственных информационных систем	6	4		4							
Тема 4. Порядок разработки, согласования и утверждения планов проведения мероприятий по защите государственных информационных систем. Создание и функционирование системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий. Стадии и этапы создания системы защиты государственных информационных систем (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты	6	4		4			8				ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4

информации в ходе эксплуатации объекта информатизации). Разработка эксплуатационной документации на систему защиты информации.											
Раздел 5. Интеллектуальная собственность	6			4							
Тема 5. Интеллектуальная собственность и история ее правовой охраны в России. Правовое регулирование авторских прав и прав, смежных с авторскими. Патентное право. Международные соглашения в области охраны интеллектуальной собственности. Право на использование объектов интеллектуальной собственности, составляющих единую технологию. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам (Роспатент): правовая основа деятельности, структура, функции. Права на программы для ЭВМ и базы данных. Понятие и правовой режим программ для ЭВМ и баз данных. Субъекты прав на программы для ЭВМ и базы данных. Содержание прав на программы для ЭВМ и базы данных. Исключительное право	6	4		4							ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4

на программу для ЭВМ или базу данных, созданную по договору заказа либо при выполнении работ по договору подрядного типа											
Контактная работа	6	18		18						2	x
Самостоятельная работа	6						28		6		x
Объем дисциплины в семестре	6	18		18			28		6	2	x
Тема 6. Коммерческая тайна. Сущность, задачи и особенности защиты коммерческой тайны. Меры по обеспечению защиты коммерческой тайны. Классификация мер защиты коммерческой тайны. Ответственность за нарушение коммерческой тайны.	7	2		4					20		ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4
Тема 7. Служебная тайна. Профессиональная тайна. Тайна следствия и судопроизводства. Отличие служебной тайны от профессиональной. Требования к защите служебной и профессиональной тайны. Ответственность за нарушение области защиты служебной и профессиональной тайн.	7	2		4				10			ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4
Раздел 8. Режим защиты государственной тайны	7	12		26							

Тема 8. Степени секретности сведений и грифы секретности носителей этих сведений. Органы защиты государственной тайны. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне. Межведомственная комиссия по защите государственной тайны. Полномочия. Обеспечение деятельности. Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны. Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.	7	12		26					24		ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-2.4, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4
Контактная работа	7	16		34						4	x
Самостоятельная работа	7							10	44		x
Объем дисциплины в семестре	7	16		34				10	44	4	x
Всего по дисциплине		34		52			28	10	50	6	

5.2. Темы курсовых работ (проектов)

Не предусмотрено

5.3. Темы индивидуальных домашних заданий (контрольных работ)

Вопросы для опроса

Роль и место информационной безопасности в системе национальной безопасности Российской Федерации

1. Место информационной безопасности в общей системе безопасности РФ.
2. Основные задачи государственной системы защиты информации.
3. Организационная структура государственной системы защиты информации.
4. Функциональная структура государственной системы защиты информации.
5. Что такое Доктрина ИБ РФ?
6. Перечислите основные составляющие национальных интересов РФ в информационной сфере.
7. Дайте определение ИБ.
8. Сформулируйте интересы государства, общества и личности в информационной сфере.
9. Сформулируйте основные направления международного сотрудничества Российской Федерации в области ИБ.
10. Перечислите основные функции системы обеспечения ИБ.
11. Как подразделяются общие методы обеспечения ИБ?
12. Каковы особенности обеспечения ИБ РФ в сферах экономики, внешней политики, внутренней политики, областях науки и техники, сфере духовной жизни, информационных и телекоммуникационных системах, в сфере обороны, правоохранительной и судебной сферах, в условиях чрезвычайных ситуаций?
13. В чем заключаются национальные интересы и безопасность РФ.
14. Сформулируйте определение безопасности в соответствии с Федеральным законом №390 «О безопасности».
15. Назовите основные принципы обеспечения безопасности.
16. Какие риски и угрозы несет несоблюдение экономической, политической, социальной, экологической, военной, культурной, информационной безопасностей?
17. В каком документе отражена задача укрепления информационной безопасности?
18. Какие сложности возникают при решении задачи по обеспечению защиты граждан и государства в информационной сфере?
19. Какие задачи информационной безопасности должны быть решены на период до 2020 года?
20. Какие существуют методы обеспечения информационной безопасности в соответствии с Доктриной информационной безопасности? Что они в себя включают?
21. Дайте определение терминам «информационные технологии», «обладатель информации», «доступ к информации», «документированная информация», «защита информации», «за-щита информации от утечки», «защита информации от преднамеренного воздействия», «защита информации от НСД», «техническая защита конфиденциальной информации», «система защиты информации», «средство защиты информации», «средство контроля эффективности защиты информации», «объект информатизации», «защищаемый объект информатизации», «основные технические средства и системы», «вспомогательные технические средства и системы», «защищаемые помещения», «лицензирование», «сертификация», «аттестация объектов информатизации», «неотказуемость», «подотчетность», «аутентичность», «достоверность».
22. Правовая защита – направление защиты информации. Государственное регулирование информационной безопасности. Доктрина информационной безопасности РФ.
23. Организационная защита – направление защиты информации. Содержание основных организационных мероприятий. Функционал службы защиты информации.
24. Инженерно-техническая защита – направление защиты информации. Классификация средств инженерно-технической защиты. Краткая характеристика основных классов.

Государственная система правового обеспечения защиты информации в Российской Федерации

1. К каким последствиям может привести утрата конфиденциальной информации.
2. От кого Вы защищаете конфиденциальную информацию.
3. Что называется коммерческой тайной?
4. Что такое служебная тайна?
5. Что представляет профессиональная тайна?
6. Что такое информация ограниченного распространения?
7. Каковы виды доступа к информации?
8. Что такое персональные данные?
9. Что такое конфиденциальная информация, государственная и коммерческая тайна?
10. Назовите три категории ценности коммерческой информации.
11. Что такое товарная ценность информации и каковы пути ее получения?
12. На основе, каких документов проводится анализ информационных активов предприятия?
13. Какие виды информации ограниченного доступа Вы знаете? Перечислите их.
14. Перечислите функции каждой организации структуры органов власти по защите информации, представленной на рисунке
15. Что такое Коммерческая тайна? Что нельзя отнести к коммерческой тайне?
16. Что такое служебная информация? Какие виды информации Вы можете отнести к служебной тайне?
17. Что такое профессиональная тайна? Какие виды информации Вы можете отнести к профессиональной тайне?
18. Что такое интеллектуальная собственность? Какие виды информации Вы можете отнести к интеллектуальной собственности?
19. Что такое активы предприятия? Что такое информационные активы? Как правильно их проанализировать?
20. Понятие и виды информации, защищаемой законодательством Российской Федерации. Основные концептуальные положения системы защиты информации.
21. Правовое регулирование технологического обмена. Защита интеллектуальной собственности. Критерии ценности документов.
22. Предпосылки к разглашению сведений, составляющих коммерческую тайну. Экспертиза ценности документов.
23. Назовите основные мероприятиями по защите от разглашения конфиденциальной информации.

Защита персональных данных

Регуляторы в области защиты ПДн.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации.

Требования к защите персональных данных при их обработке в информационных системах персональных данных.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

Ответственность за нарушение обработки ПДн.

Ответственность за нарушение режима защиты персональных данных.

2. Создание и функционирование системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.

3. Стадии и этапы создания системы защиты государственных информационных систем (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).

4. Разработка эксплуатационной документации на систему защиты информации.

Интеллектуальная собственность

1. Интеллектуальная собственность и история ее правовой охраны в России.
2. Правовое регулирование авторских прав и прав, смежных с авторскими.
3. Патентное право.
4. Международные соглашения в области охраны интеллектуальной собственности.
5. Право на использование объектов интеллектуальной собственности, составляющих единую технологию.
6. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам (Роспатент): правовая основа деятельности, структура, функции.
7. Права на программы для ЭВМ и базы данных.
8. Понятие и правовой режим программ для ЭВМ и баз данных.
9. Субъекты прав на программы для ЭВМ и базы данных.
10. Содержание прав на программы для ЭВМ и базы данных.
11. Исключительное право на программу для ЭВМ или базу данных, созданную по договору заказа либо при выполнении работ по договору подрядного типа

Режим защиты коммерческой тайны

1. Коммерческая тайна.
2. Сущность, задачи и особенности защиты коммерческой тайны. Меры по обеспечению защиты коммерческой тайны.
3. Работа с информацией, составляющей коммерческую тайну.
4. Коммерческая тайна в трудовых отношениях.
5. Классификация мер защиты коммерческой тайны.
6. Ответственность за нарушение коммерческой тайны.

Служебная и профессиональная тайны. Тайна следствия и судопроизводства.

1. Служебная тайна.
2. Профессиональная тайна.
3. Тайна следствия и судопроизводства.
4. Отличие служебной тайны от профессиональной.
5. Требования к защите служебной и профессиональной тайны.
6. Ответственность за нарушение режима защиты служебной тайны.
7. Ответственность за нарушение режима защиты профессиональной тайны.
8. Ответственность за нарушение тайны следствия и судопроизводства.

Режим защиты государственной тайны

1. Что такое государственная тайна?
2. Назовите три степени секретности.
3. Понятие государственной тайны.

4. Полномочия органов государственной власти в области защиты государственной тайны.

5. Порядок отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

6. Допуск к государственной тайне.

7. Защита государственной тайны.

8. Концептуальные основы защиты государственной тайны.

9. Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.

10. Реквизиты носителей сведений, составляющих государственную тайну.

11. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

12. Основные классы документов по защите государственной тайны: правовые; организационно-распорядительные; нормативные; плановые; информационные.

13. Органы государственной власти, предприятия, учреждения, организации и их структурные подразделения по защите государственной тайны

14. Порядок допуска должностных лиц и граждан к государственной тайне.

15. Особенности допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов, к государственной тайне.

16. Особый порядок допуска к государственной тайне.

17. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне.

18. Организация защиты информации, составляющей государственную тайну, на предприятиях, в организациях и учреждениях.

19. Особенности защиты информации в условиях реализации международных договоров по сокращению вооружений и вооруженных сил.

20. Особенности защиты информации в условиях создания совместных предприятий.

21. Особенности защиты информации в условиях научно-технического, военно-технического и экономического сотрудничества с другими странами.

5.4 Вопросы для самостоятельного изучения по очной форме обучения

№ п.п.	Наименования темы	Наименование вопросов	Объем, академические часы
1	Служебная тайна. Профессиональная тайна. Тайна следствия и судопроизводства. Отличие служебной тайны от профессиональной. Требования к защите служебной и профессиональной тайны. Ответственность за нарушение области защиты служебной и профессиональной тайн.	Конституция Российской Федерации о защите государственной тайны. Особенности допуска к государственной тайне лиц, имеющих двойное гражданство, апатридов, иностранных граждан, эмигрантов и реэмигрантов. Отличие служебной тайны от профессиональной. Технические средства защиты информации и их применение в области защиты государственной тайны. Государственная политика информационной безопасности и организационная основа ее обеспечения.	10

		Особенности защиты государственной тайны в условиях реализации международных договоров по сокращению вооружений и вооруженных сил. Особенности защиты государственной тайны в условиях создания совместных предприятий. Ответственность за нарушение области защиты служебной и профессиональной тайн.	
		Всего	10

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1.Крыжановский, А. В. Организационное и правовое обеспечение информационной безопасности : методические указания / А. В. Крыжановский. — Самара : ПГУТИ, 2018. — 56 с. — Текст : электронный // Лань : электронно-библиотечная система.

2. Масюк, М. А. Основные понятия и правовые основы защиты информации : учебное пособие / М. А. Масюк, А. А. Попов, Е. В. Касьянова. — Красноярск :СибГУ им. академика М. Ф. Решетнёва, 2020. — 82 с. — Текст : электронный // Лань : электронно-библиотечная система.

3. Груздева, Л. М. Основы информационной безопасности : учебное пособие : в 2 частях / Л. М. Груздева. — Москва : РУТ (МИИТ), 2017 — Часть 1 — 2017. — 101 с. — Текст : электронный // Лань : электронно-библиотечная система.

4. Куликова, С. А. Информационное право : учебное пособие / С. А. Куликова. — Саратов : СГУ, 2020. — 92 с. — ISBN 978-5-292-04670-7. — Текст : электронный // Лань : электронно-библиотечная система.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1.Организационно-правовое обеспечение информационной безопасности : учебник / А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев; под редакцией А. А. Александрова, М. П. Сычева. — Москва : МГТУ им. Баумана, 2018. — 291 с. — ISBN 978-5-7038-4723-7. — Текст : электронный // Лань : электронно-библиотечная система.

2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система.

3. Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамееева. — Санкт-Петербург :СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с. — ISBN 978-5-89160-213-7. — Текст : электронный // Лань : электронно-библиотечная система.

4. Мызникова, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Мызникова. — Омск :ОмГУПС, 2017. — 82 с. — ISBN 978-5-949-41160-5. — Текст : электронный // Лань : электронно-библиотечная система.

5. Пашкова, Н. Н. Основы регулирования инновационной деятельности : учебное пособие / Н. Н. Пашкова, Р. Н. Салиева. — Тюмень :ТюмГНГУ, 2012. — 194 с. — ISBN 978-5-9961-0593-9. — Текст : электронный // Лань : электронно-библиотечная система.

6.3 Методические материалы для обучающихся по освоению дисциплины

Тематическое содержание дисциплины

7. Требования к материально-техническому и учебно-методическому содержанию дисциплины

7.1 Учебные аудитории для проведения учебных занятий по дисциплине

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации, укомплектованной специализированной мебелью и техническими средствами обучения.

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.
Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованных специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования

7.2 Перечень оборудования и технических средств обучения по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиа -проектором, компьютером и учебной доской.

7.3 Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. JoliTest (JTRun, JTEditor, TestRun)
2. MS Office

7.4 Современные профессиональные базы данных и информационно-справочные системы

1. Консультант +.

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Доцент,к.т.н. _____ Фот Юлия Дмитриевна

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович

Программа рассмотрена и утверждена на заседании Ученого совета Института управления рисками и комплексной безопасности, протокол № 4 от 22.01.2021 г.

Директор Института управления рисками и комплексной безопасности

_____ Яковлева Евгения Васильевна

Дополнения и изменения

в рабочей программе дисциплины Б1.О.06 Организационное и правовое обеспечение информационной безопасности на 2021- 2022 учебный год.

В программу вносятся следующие изменения: без изменений

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 19.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович