

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

СОГЛАСОВАНО

Декан ФИТ

А.С. Авдеев

Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.О.29 «Организационное и правовое обеспечение информационной безопасности»**

Код и наименование направления подготовки (специальности): **10.03.01**

Информационная безопасность

Направленность (профиль, специализация): **Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)**

Статус дисциплины: **обязательная часть**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	доцент	А.В. Санников
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	Е.В. Шарлаев

г. Барнаул

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1	Анализирует поставленную цель и формулирует задачи, которые необходимо решить для её достижения
		УК-2.2	Выбирает оптимальный способ решения задач с учётом существующих ресурсов и ограничений
		УК-2.3	Выбирает правовые и нормативно-технические документы, применяемые для решения поставленных задач
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1	Осуществляет поиск необходимых нормативных правовых актов и нормативных методических документов
		ОПК-5.2	Демонстрирует знание состава нормативной документации
		ОПК-5.3	Использует нормативные правовые акты, нормативные методические документы в профессиональной деятельности
ОПК-6	Способен при решении профессиональных задач организовать 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	Выбирает нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Документоведение, Основы информационной безопасности
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации, Основы управления информационной безопасностью, Разработка организационно-распорядительной документации по защите информации

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 6 / 216

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	32	0	64	120	109

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Форма обучения: очная

Семестр: 3

Объем дисциплины в семестре з.е. /час: 2 / 72

Форма промежуточной аттестации: Зачет

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
16	0	32	24	52

Лекционные занятия (16ч.)

1. Правовые основы в области ИБ {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.) [1,4,5,6,7,9,10]

Информационная сфера и информация в системе права. Основные понятия права. Информационная сфера как предмет правового регулирования. Информация как объект права и защиты. Системы обработки, хранения и передачи информации как объекты права. Содержание и структура правового обеспечения информационной безопасности. Роль права в регулировании комплекса отношений в области информационной безопасности. Понятие, предмет и содержание правового обеспечения информационной безопасности. Принципы правового регулирования отношений, связанных с обеспечением информационной безопасности.

Структура законодательства в области информационной безопасности, состав нормативной документации. Основные законодательные акты по видам защиты информации. Использование нормативных правовых актов, нормативных методических документы в профессиональной деятельности. Правовые основы защиты информации. Принципы правового регулирования отношений по защите информации. Цели и задачи защиты информации. Правовая защита информации

ограниченного доступа. Правовой режим защиты информации. Ответственность за правонарушения в области защиты информации. Правовые основы деятельности и функции органов, обеспечивающих информационную безопасность. Органы, обеспечивающие информационную безопасность в Российской Федерации. Межведомственные комиссии. Федеральная служба безопасности России. Федеральная служба по техническому и экспортному контролю.

2. Правовые режимы {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[1,4,5,6,7] Лицензирование и сертификации в области защиты информации. Основные понятия и источники права по лицензированию в области защиты информации. Лицензируемые виды деятельности. Сертификация средств защиты информации.

Государственная тайна как объект права. Отнесение сведений к государственной тайне, их засекречивание и рассекречивание. Распоряжение информацией, составляющей государственную тайну. Режим и органы защиты государственной тайны. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну. Правовая основа допуска должностных лиц и граждан к государственной тайне. Контроль и надзор за обеспечением защиты государственной тайны.

Коммерческая тайна как объект права. Отнесение информации к ИСКТ. Охрана конфиденциальности информации. Режим коммерческой тайны. Субъекты права на коммерческую тайну и их обязанности по охране конфиденциальности ИСКТ. Нормативное правовое обеспечение режима коммерческой тайны организации.

Персональные данные как особый институт охраны права на неприкосновенность частной жизни. Персональные данные как объект права и защиты. Субъекты правоотношений связанных с обработкой персональных данных их права и обязанности. Обеспечение безопасности персональных данных при их обработке.

3. Правовые вопросы в сфере информационной безопасности {с элементами электронного обучения и дистанционных образовательных технологий} (4ч.)[1,5,6,8,9,10] Понятие интеллектуальной деятельности и интеллектуального продукта. Институты права и объекты интеллектуальной собственности. Интеллектуальные права. Распоряжение исключительным правом. Защита интеллектуальных прав.

Преступления в сфере компьютерной информации. Классификация компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание и распространение вредоносных программ для ЭВМ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Правовая ответственность за нарушения законодательства о государственной тайне. Виды правовой ответственности за нарушения законодательства о государственной тайне. Виды посягательств на государственную тайну. Уголовная ответственность за посягательства на государственную тайну. Административная и дисциплинарная ответственность за нарушения в области защиты государственной тайны. Правовая ответственность за нарушения законодательства о тайнах и об интеллектуальной собственности.

Ответственность за нарушение законодательства о коммерческой тайне.
Ответственность за нарушение законодательства о персональных данных.
Ответственность за нарушение законодательства о служебной и профессиональной тайне. Ответственность за нарушение законодательства об интеллектуальной собственности.

Практические занятия (32ч.)

- 1. Информационная сфера и информация в системе права {дискуссия} (3ч.)[1,5,6,7]** Информация как объект права и защиты. Системы обработки, хранения и передачи информации как объекты права.
- 2. Структура правового обеспечения информационной безопасности {дискуссия} (2ч.)[1,5,6,7]**
- 3. Законодательство в области информационной безопасности {дискуссия} (4ч.)[1,5,6,7]** Основные законодательные акты по видам защиты информации. Технологии поиска необходимых нормативных правовых актов и нормативных методических документов.
- 4. Правовые основы защиты информации {дискуссия} (3ч.)[1,5,6,7]** Цели и задачи защиты информации. Правовая защита информации ограниченного доступа.
- 5. Правовые основы деятельности и функции органов, обеспечивающих информационную безопасность {дискуссия} (4ч.)[1,5,6,7,9,10]** Деятельность межведомственных комиссий, ФСБ России, ФСТЭК России.
- 6. Лицензирование и сертификация в области защиты информации {дискуссия} (2ч.)[1,7]**
- 7. Правовой институт государственной тайны {дискуссия} (2ч.)[1,6,9]**
- 8. Правовой институт коммерческой тайны {дискуссия} (2ч.)[1,5,6]**
- 9. Правовой институт персональных данных {дискуссия} (2ч.)[1,6,12]**
- 10. Правовое регулирование интеллектуальной собственности {дискуссия} (2ч.)[1,5,6,7]**
- 11. Преступления в сфере компьютерной информации {дискуссия} (2ч.)[1,5,6,7]**
- 12. Правовая ответственность за нарушения законодательства Российской Федерации о государственной тайне {дискуссия} (2ч.)[1,5,6,11]**
- 13. Правовая ответственность за нарушения законодательства о тайнах и об интеллектуальной собственности {дискуссия} (2ч.)[1,6]**

Самостоятельная работа (24ч.)

- 1. Подготовка к текущим занятиям(14ч.)[1,5,6,7,8,9,10,11,12]**
- 2. Подготовка к зачету(10ч.)[1,5,6,7,8,9,10,11,12]**

Семестр: 4

Объем дисциплины в семестре з.е. /час: 4 / 144

Форма промежуточной аттестации: Экзамен

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
16	0	32	96	57

Лекционные занятия (16ч.)

1. Сущность организационного обеспечения информационной безопасности {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[2,4,5,8] Сущность организационного обеспечения информационной безопасности. Организация работы по определению состава, засекречиванию и рассекречиванию информации. Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности. Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. Организация системы доступа к защищаемой информации (сведениям, документам, изделиям).

2. Организационная деятельность на предприятии(5ч.)[2,4,5,8] Анализ поставленной цели защиты информации и формулировка задач, которые необходимо решить для её достижения. Работа с персоналом, имеющим допуск и доступ к конфиденциальной информации. Организация охраны предприятия и физической защиты его объектов. Организация пропускного и внутриобъектового режимов. Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями. Выбор правовых и нормативно-технических документов, применяемых для решения поставленных задач, в том числе нормативных правовых актов, нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

3. Организация защиты информации(5ч.)[2,4,5,8] Выбор оптимальных способов решения задач защиты информации с учётом существующих ресурсов и ограничений. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности. Защита информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу. Организация служебного расследования по фактам разглашения конфиденциальной информации или утраты носителей информации.

Практические занятия (32ч.)

1. Сущность организационного обеспечения информационной безопасности {дискуссия} (2ч.)[2,4,8] Место организационной защиты информации в системе комплексной защиты информации. Основные направления, принципы и условия

организационной защиты информации. Основные методы, силы и средства, используемые для организации защиты информации

2. Организация работы по определению состава, засекречиванию и рассекречиванию информации {дискуссия} (3ч.)[2,4,8] Отнесение сведений к различным видам конфиденциальной информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей. Отнесение сведений к коммерческой тайне. Реквизиты носителей.

3. Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности {дискуссия} (3ч.)[2,4,8] Основные положения лицензирования деятельности предприятий в области защиты государственной тайны. Организация и проведение специальных экспертиз предприятий (организаций). Организация проведения государственной аттестации руководителей предприятий

4. Определение должностей и подбор персонала для работы с конфиденциальной информацией {дискуссия} (3ч.)[2,4,8] Оформление допуска граждан к государственной тайне. Особенности подбора персонала на должности, связанные с конфиденциальной информацией. Состав документов. Основные положения допуска должностных лиц и граждан к государственной тайне. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа лицу в допуске к государственной тайне и условия прекращения допуска.

5. Организация системы доступа к защищаемой информации {дискуссия} (3ч.)[2,4,8] Организация доступа персонала предприятия к сведениям, составляющим государственную тайну, и их носителям. Порядок доступа к конфиденциальной информации командированных лиц. Разрешительная система доступа персонала к конфиденциальной информации.

6. Работа с персоналом, имеющим допуск и доступ к конфиденциальной информации {дискуссия} (2ч.)[2,4,8] Основы работы с персоналом предприятия. Основные этапы работы с персоналом. Методы работы с персоналом и их характеристика.

7. Организация охраны предприятия и физической защиты его объектов {дискуссия} (2ч.)[2,4,8]

8. Организация пропускного и внутриобъектового режимов {дискуссия} (2ч.)[2,4,8] Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства. Работа по организации внутриобъектового режима. Основные подходы и принципы. Силы и средства, используемые при организации внутриобъектового режима

9. Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями {дискуссия} (2ч.)[2,4,8]

10. Организация подготовки и проведения совещаний и переговоров по

конфиденциальным вопросам {дискуссия} (3ч.)[2,4,8] Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов

11. Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности {дискуссия} (3ч.)[2,4,8] Общие положения. Организация защиты информации в ходе проведения мероприятий рекламного характера. Защита информации при осуществлении публикаторской деятельности. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации при взаимодействии со СМИ.

12. Защита информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу {дискуссия} (2ч.)[2,4,8] Общие положения. Организация подготовки к передаче другим государствам сведений, составляющих государственную тайну. Организация защиты информации при приеме на предприятии иностранных представителей. Порядок выезда персонала, осведомленного в сведениях, составляющих государственную тайну, за границу.

13. Организация служебного расследования по фактам разглашения конфиденциальной информации или утраты носителей информации {дискуссия} (2ч.)[2,4,8] Ответственность за разглашение конфиденциальной информации и утрату носителей информации. Организация и проведение служебного расследования по фактам нарушения. Формирование, организация и поддержка выполнения комплекса мер по обеспечению информационной безопасности.

Самостоятельная работа (96ч.)

1. Подготовка к текущим занятиям(35ч.)[2,5,6,7,8]

2. Написание курсовой работы(25ч.)[2,3,5,8]

3. Подготовка к экзамену(36ч.)[2,3,5,8]

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Загинайлов Ю. Н. Организационно-правовое обеспечение информационной безопасности. В 2-х частях. Часть I. Правовое обеспечение информационной безопасности : Учебное пособие / Алт.гос.техн.ун-т им.И.И.Ползунова.- Баранаул: Изд-во АлтГТУ.-2012-172с. Прямая ссылка: <http://elib.altstu.ru/eum/download/vsib/zaginajlov-opobespet.pdf>

2. Загинайлов Ю. Н. Организационно-правовое обеспечение информационной безопасности. В 2-х частях. Часть II. Организационное обеспечение информационной безопасности : курс визуальных лекций / Алт.гос.техн.ун-т им.И.И.Ползунова.- Барнаул: Изд-во АлтГТУ.-2014-106с. -режим доступа: <http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-585a20f755ca5.pdf>

3. Загинайлов Ю.Н. Методические рекомендации по выполнению курсовых работ по дисциплине «Организационно-правовое обеспечение информационной безопасности» / Ю.Н. Загинайлов; АлтГТУ. – Барнаул, 2012.- 30с. -11 экз.

4. Загинайлов Ю.Н. Методические рекомендации к семинарским (практическим) занятиям и указания к СРС по дисциплине «Организационно-правовое обеспечение информационной безопасности. Часть 2. Организационное обеспечение информационной безопасности »/Алт.гос.техн.ун-т им.И.И.Ползунова.- 2014- 123 с. [электронный ресурс]: -Прямая ссылка: <http://elib.altstu.ru/eum/download/vsib/Zaginajlov-sz2.pdf>

6. Перечень учебной литературы

6.1. Основная литература

5. Аверченков, В. И. Служба защиты информации: организация и управление : [16+] / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 186 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=93356> (дата обращения: 08.06.2021). – Библиогр. в кн. – ISBN 978-5-9765-1271-9. – Текст : электронный.

6. Лапина, М. А. Информационное право : учебное пособие / М. А. Лапина, А. Г. Ревин, В. И. Лапин ; ред. И. Ш. Килясханов. – Москва : Юнити, 2015. – 336 с. – (Высшее профессиональное образование: Юриспруденция). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=118624> (дата обращения: 08.06.2021). – Библиогр. в кн. – ISBN 5-238-00798-1. – Текст : электронный.

6.2. Дополнительная литература

7. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5163

8. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие : [16+] / Е. Н. Чекулаева, Е. С. Кубашева ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2020. – 156 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612591> (дата обращения: 08.06.2021). – Библиогр.: с. 127-129. – ISBN 978-5-8158-2165-1. – Текст : электронный.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

9. Официальный сайт Совета Безопасности Российской Федерации
<http://www.scrf.gov.ru/>

10. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России <https://fstec.ru/>

11. Официальный сайт Федеральной службы безопасности (ФСБ) России
<http://www.fsb.ru>

12. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
<https://rkn.gov.ru>

8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

№пп	Используемое программное обеспечение
1	LibreOffice
2	Microsoft Office
3	Windows
4	Антивирус Kaspersky
5	(БТИ) КонсультантПлюс
6	Гарант
7	Яндекс.Браузер

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные

№пп	Используемые профессиональные базы данных и информационные справочные системы
	интернет-ресурсы (http://Window.edu.ru)
2	Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/)

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы
учебные аудитории для проведения учебных занятий
помещения для самостоятельной работы

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».