

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.Б.20 «Организационное и правовое обеспечение информационной безопасности»**

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

Информационная безопасность

Направленность (профиль, специализация): **Организация и технология защиты информации**

Статус дисциплины: **обязательная часть (базовая)**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	ассистент	В.К. Николаева
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 планируемыми результатами освоения образовательной программы

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
ОПК-5	способностью использовать нормативные правовые акты в профессиональной деятельности	основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области информационной безопасности и защиты информации; основы работы с документами, в том числе в области организационного и правового обеспечения информационной безопасности	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	навыками работы с нормативными правовыми актами в области ИБ
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	принципы формирования комплекса мер по обеспечению информационной безопасности, в том числе в области организационного и правового обеспечения	разрабатывать комплекс мер по обеспечению информационной безопасности	методами разработки комплекса мер по обеспечению информационной безопасности

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Основы информационной безопасности, Правоведение
---	--

Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексное обеспечение защиты информации объекта информатизации, Нормативные акты и стандарты по информационной безопасности, Основы управления информационной безопасностью
---	---

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	51	0	51	114	114

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

Форма обучения: очная

Семестр: 5

Объем дисциплины в семестре з.е. /час: 3 / 108

Форма промежуточной аттестации: Зачет

Лекции	Виды занятий, их трудоемкость (час.)			Объем контактной работы обучающегося с преподавателем (час)
	Лабораторные работы	Практические занятия	Самостоятельная работа	
34	0	17	57	60

Лекционные занятия (34ч.)

1. Правовые основы в области ИБ {с элементами электронного обучения и дистанционных образовательных технологий} (12ч.)[1,5] 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 и содержание законодательства в области информационной безопасности. Структура законодательства в области информационной безопасности. Содержание законодательства в области информационной безопасности. Основные законодательные акты по видам защиты информации.

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} (12ч.)[1,6] Правовые режимы лицензирования и сертификации в области защиты информации. Основные понятия и источники права по лицензированию в области защиты информации. Лицензируемые виды деятельности. Сертификация средств защиты информации. Системы сертификации.

Правовой режим государственной тайны. 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.

Правовой режим коммерческой 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.

Правовой режим персональных данных. 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 ИБ {с элементами электронного обучения и дистанционных образовательных технологий} (10ч.)[1] Основные понятия, принципы и институты правового регулирования интеллектуальной собственности. Понятие интеллектуальной деятельности и интеллектуального продукта. Институты права и объекты интеллектуальной собственности.

Интеллектуальные права. Распоряжение исключительным правом. Защита интеллектуальных прав.

Правовые средства противодействие преступлениям 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 Российской Федерации 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 (17ч.)

1. Правовые основы в области ИБ {дискуссия} (8ч.)[3] Информационная сфера и информация в системе права. Структура и содержание законодательства в области информационной безопасности. Правовые основы защиты информации. Правовые основы деятельности и функции органов, обеспечивающих информационную безопасность.

2. Правовые режимы {дискуссия} (6ч.)[3,5] Правовой режим государственной тайны. Правовой режим коммерческой тайны. Правовой режим персональных данных

3. Правовая ответственность за нарушения законодательства Российской Федерации о государственной тайне. {дискуссия} (3ч.)[3,10] 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.

Курсовые работы (20ч.)

. Курсовая работа(20ч.)[4,5,6,7,8,9,10]

Самостоятельная работа (57ч.)

1. Подготовка к промежуточной аттестации (зачёт)(12ч.)[1,5]
2. Подготовка к текущим занятиям, самостоятельное изучение материала(16ч.)[1,3,10]
3. Выполнение курсовой работы(20ч.)[8,9,10]
4. Подготовка к текущему контролю успеваемости(9ч.)[1,5,10]

Семестр: 6

Объем дисциплины в семестре з.е. /час: 3 / 108

Форма промежуточной аттестации: Экзамен

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
17	0	34	57	54

Лекционные занятия (17ч.)

1. **Организационное обеспечение ИБ {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[2,7]** 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 для обеспечения ИБ {с элементами электронного обучения и дистанционных образовательных технологий} (5ч.)[2,7]** 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.
3. **Организация ЗИ {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[2]** 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 (34ч.)

1. **Организационная деятельность на предприятии для обеспечения**

ИБ(12ч.)[2] Сущность организационного обеспечения информационной безопасности. 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.

Организация работы по определению состава, засекречиванию и рассекречиванию информации. 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 сведений.

Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности. Основные положения лицензирования деятельности предприятий в области защиты государственной тайны. Организация и проведение специальных экспертиз предприятий (организаций). Организация проведения государственной аттестации руководителей предприятий.

Определение должностей и подбор персонала для работы с конфиденциальной информацией. 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.

Организация системы доступа к защищаемой информации (сведениям, документам, изделиям). 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.

2. Организация ЗИ(10ч.)[2] Работа с персоналом, имеющим допуск и доступ к конфиденциальной информации. Основы работы с персоналом предприятия. Основные этапы работы с персоналом. Методы работы с персоналом и их характеристика.

Организация охраны предприятия и физической защиты его объектов. Организация охраны предприятия. Физическая защита объектов предприятия.

Организация пропускного и внутриобъектового режимов. 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.

Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями

3. Организационное обеспечение ИБ(12ч.)[2,4] Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. 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.

Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности. 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.

Защита информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу. 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.

Организация служебного расследования по фактам разглашения конфиденциальной информации или утраты носителей информации. 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 (57ч.)

1. Подготовка к текущим занятиям, самостоятельное изучение материала(12ч.)[2,8,9,10,11]

2. Подготовка к текущему контролю успеваемости(9ч.)[2]

3. Подготовка к промежуточной аттестации (экзамен)(36ч.)[1,2]

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. Правовое обеспечение информационной безопасности: Учебное пособие. Ч. 1 /Ю. Н. Загинайлов.- Барнаул : Изд-во АлтГТУ , 2012 - 172 с. - Режим доступа:

<http://new.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. [Электронный ресурс]: -режим доступа: <http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-585a20f755ca5.pdf>

3. Загинайлов Ю.Н. Методические рекомендации к семинарским занятиям и указания к СРС по дисциплине «Организационно и правовое обеспечение информационной безопасности. Часть 1. Правовое обеспечение информационной безопасности »/ Алт.гос.техн.ун-т им.И.И.Ползунова.- 2019- 76с. [электронный ресурс]: -режим доступа: <http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-5c4a9aea2ffb9.pdf>

6. Перечень учебной литературы

6.1. Основная литература

4. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93356>

5. Лапина, М.А. Информационное право : учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин ; под ред. И.Ш. Килясханова. - М. : Юнити-Дана, 2015. - 336 с. - (Высшее профессиональное образование: Юриспруденция). - Библиогр. в кн. - ISBN 5-238-00798-1 ; То же [Электронный ресурс]. - URL: <https://biblioclub.ru/index.php?page=book&id=118624>

6.2. Дополнительная литература

6. 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 — Загл. с экрана.

7. Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учебник для студ. высш. учеб. заведений / О. А. Романов, С. А. Бабин, С. Г. Жданов. – М. : Академия, 2008. – 192 с. (Гриф УМО-25 экз.)

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

8. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: <http://www.fstec.ru>.

9. Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: <http://protect.gost.ru/>

10. Правовая справочная система «Гарант» [электронный ресурс]: -режим доступа: <http://www.garant.ru>

11. Официальный сайт Совета Безопасности Российской Федерации <http://www.scrf.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	Chrome
2	Windows
3	Гарант
4	LibreOffice
5	Антивирус Kaspersky

№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 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 занятий лекционного типа
учебные аудитории для проведения занятий семинарского типа
учебные аудитории для проведения курсового проектирования (выполнения курсовых работ)
учебные аудитории для проведения групповых и индивидуальных консультаций
учебные аудитории для проведения текущего контроля и промежуточной аттестации
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».