

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.В.ДВ.1.1 «Правовое обеспечение компьютерной безопасности»**

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

Информационная безопасность

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

Статус дисциплины: **дисциплины (модули) по выбору**

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	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности применительно к компьютерной безопасности	навыками работы с нормативными правовыми актами в области компьютерной безопасности
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации.	организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю, в том числе в области компьютерной безопасности	

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики),	Документоведение, Организационное и правовое обеспечение информационной безопасности, Основы
------------------------	----------------------------------------------------------------------------------------------

предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	информационной безопасности
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Информационная безопасность автоматизированных систем, 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: 2 / 72

Форма промежуточной аттестации: Зачет

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	17	0	17	38	40

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

Форма обучения: очная

Семестр: 7

Лекционные занятия (17ч.)

1. Компьютерные преступления {с элементами электронного обучения и дистанционных образовательных технологий} (8ч.)[2] 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

Особенности квалификации компьютерных преступлений. Криминалистическая характеристика преступлений в сфере компьютерной информации. Международный характер компьютерных преступлений. Доказательство в

судебных делах по компьютерным преступлениям. Особенности расследования компьютерных преступлений. Методика раскрытия и расследования компьютерных преступлений. Типичные следственные ситуации первоначального этапа и следственные действия. Особенности производства осмотров и обысков. Поиск и изъятие информации и следов воздействия на нее в ЭВМ и ее устройства. Использование специальных познаний и назначение экспертиз.

2. Способы защиты от компьютерных преступлений {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[1] Институт электронной подписи. История возникновения института ЭП. Основные понятия, используемые в законе. Электронные подписи и их использование. Удостоверяющие центры их функции. Квалифицированный сертификат и его выдача Институт авторского права в системе компьютерной безопасности. История становления института авторского права в России. Объекты и субъекты авторского права. Авторские права. Исключительное право на произведение. Свободное воспроизведение произведения. Программы для ЭВМ и базы данных как объекты защиты авторского права. Защита авторских прав.

3. Правовое регулирование отношений в сети Интернет. {с элементами электронного обучения и дистанционных образовательных технологий} (3ч.)[1] Субъекты и объекты правоотношений в сети Интернет. Общественное регулирование отношений в сети Интернет. Основные вопросы, требующие правового регулирования отношений в сети Интернет. Законодательство, связанное с интернет-деятельностью. Меры по обеспечению информационной безопасности РФ при использовании ИТКС международного информационного обмена

Практические занятия (17ч.)

1. Компьютерные преступления(8ч.)[1] Преступления в сфере компьютерной информации. Неправомерный доступ к компьютерной информации. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Особенности квалификации компьютерных преступлений. Криминалистическая характеристика преступлений в сфере компьютерной информации. Международный характер компьютерных преступлений. Доказательство в судебных делах по компьютерным преступлениям. Методика раскрытия и расследования компьютерных преступлений. Типичные следственные ситуации первоначального этапа и следственные действия. Особенности производства осмотров и обысков. Поиск и изъятие информации и следов воздействия на нее в ЭВМ и ее устройства. Использование специальных познаний и назначение экспертиз. Особенности расследования компьютерных преступлений. История возникновения института ЭП. Основные понятия, используемые в законе. Электронные подписи и их использование. Удостоверяющие центры их функции. Квалифицированный сертификат и его выдача.

2. Способы защиты от компьютерных преступлений(9ч.)[1,4,5] Институт электронной подписи. Институт авторского права в системе компьютерной безопасности. Правовое регулирование отношений в сети Интернет. А также формирование умения применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности от компьютерных преступлений.

Самостоятельная работа (38ч.)

1. Подготовка к текущему контролю успеваемости(6ч.)[1,2,3]

2. Подготовка к текущим занятиям, самостоятельное изучение материала(16ч.)[1]

3. Подготовка к промежуточной аттестации (зачёт)(16ч.)[1,2,3]

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. Правовое обеспечение компьютерной безопасности: учебно-методическое пособие.-2-е изд.,испр. и доп. /Ю.Н. Загинайлов; Алт.гос.техн.ун-т им.И.И.Ползунова.- Баранаул: Изд-во АлтГТУ.- 2018 – 116 с. [электронный ресурс]: -режим доступа: <http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-5a6ae9603068e.pdf>

6. Перечень учебной литературы

6.1. Основная литература

2. Загинайлов Ю. Н. Правовое обеспечение компьютерной безопасности : курс визуальных лекций / Алт.гос.техн.ун-т им.И.И.Ползунова.- Баранаул: Изд-во АлтГТУ.-2014- 70 с. [электронный ресурс]: -режим доступа: <http://elib.altstu.ru/eum/download/vsib/ZaginU-po.pdf>

6.2. Дополнительная литература

3. Новиков, В.К. Информационное оружие – оружие современных и будущих войн [Электронный ресурс] / В.К. Новиков. — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 262 с. — Режим доступа: <https://e.lanbook.com/book/11840>. — Загл. с экрана.

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

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

5. 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 контролируемых 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 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».