федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИЧУРИНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Кафедра экономической безопасности и права

УТВЕРЖДЕНА решением учебно-методического совета университета (протокол от 23 мая 2024 г. № 09)	УТВЕРЖДАЮ Председатель учебно-методического совета университета С.В. Соловьев «23» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

И Н Ф О Р М А Ц И О Н Н О Е П Р А В О

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Системы автоматизированного проектирования

Квалификация бакалавр

Мичуринск – 2024

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) «Информационное право» является формирование у обучаемых знаний в области теоретических основ информационной безопасности и защиты информации в компьютерных комплексах, умений и навыков их практического применения, эффективного правового использования программных средств и правовой защиты информации в вычислительных системах и сетях.

2. Место дисциплины в структуре образовательной программы

Согласно учебному плану по направлению подготовки 09.03.01 Информатика и вычислительная техника дисциплина " Информационное право" является дисциплиной обязательной части Блока 1. Дисциплины (модули) (Б1.О.13).

Материал дисциплины взаимосвязан с такими дисциплинами, как: «Политология и социология», «Информатика». Знания, умения и навыки, приобретенные при изучении дисциплины (модуля) «Информационное право» необходимы при освоении дисциплин: «Информатизация научных исследований», «Защита информации». Служит базой для прохождения производственной практики по получению профессиональных умений и опыта профессиональной деятельности, защиты выпускной квалификационной работы.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование следующей компетенции:

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-10. Способен формировать нетерпимое отношение к коррупционному поведению

Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальных компетенций	Критерии оценивания результатов обучения			
		низкий (допороговый, компетенция не сформирована)	пороговый	базовый	продвинутый
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	ИД-1$_{УК-2}$ – Формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач.	Не может формулировать в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Не может определять ожидаемые результаты решения выделенных задач.	Не достаточно четко может формулировать в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Не достаточно четко может определять ожидаемые результаты решения выделенных задач.	В достаточной степени может формулировать в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Достаточно четко может определять ожидаемые результаты решения выделенных задач.	Отлично формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Четко может определять ожидаемые результаты решения выделенных задач.
	ИД-2$_{УК-2}$ – Проектирует решение конкретной задачи проекта, выбирая оптимальный	Не может проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из дей-	Не достаточно четко может проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, ис-	Достаточно хорошо может проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения,	Успешно может проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действу-

	способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений.	ствующих правовых норм и имеющихся ресурсов и ограничений.	ходя из действующих правовых норм и имеющихся ресурсов и ограничений.	исходя из действующих правовых норм и имеющихся ресурсов и ограничений.	ющих правовых норм и имеющихся ресурсов и ограничений.
	ИД-3$_{УК-2}$ – Решает конкретные задачи проекта, заявленного качества и за установленное время.	Не может решать конкретные задачи проекта, заявленного качества и за установленное время.	Слабо решает конкретные задачи проекта, заявленного качества и за установленное время.	Хорошо решает конкретные задачи проекта, заявленного качества и за установленное время.	Отлично решает конкретные задачи проекта, заявленного качества и за установленное время.
	ИД-4$_{УК-2}$ – Публично представляет результаты решения конкретной задачи проекта.	Не может публично представлять результаты решения конкретной задачи проекта.	Не уверенно публично представляет результаты решения конкретной задачи проекта.	Достаточно четко публично представляет результаты решения конкретной задачи проекта.	Олично публично представляет результаты решения конкретной задачи проекта.
УК-10. Способен формировать нетерпимое отношение к коррупционному повдению	ИД-1$_{УК-10}$Анализирует действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней	Не может анализировать действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней	Слабо анализирует действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней	Хорошо анализирует действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней	Отлично анализирует действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней
	ИД-2$_{УК-10}$Планирует, организует и проводит мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в обществе	Не может планировать, организовывать и проводить мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в обществе	Слабо может планировать, организовывать и проводить мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в обществе	Хорошо может планировать, организовывать и проводить мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в обществе	Отлично может планировать, организовывать и проводить мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в обществе
	ИД-3$_{УК-10}$Соблюдает правила общественного взаимодействия на основе нетерпимого отношения к коррупции	Не соблюдает правила общественного взаимодействия на основе нетерпимого отношения к кор-	Не полностью соблюдает правила общественного взаимодействия на основе нетерпимого отношения к кор-	Почти всегда соблюдает правила общественного взаимодействия на основе нетерпимого отношения к	Всегда соблюдает правила общественного взаимодействия на основе нетерпимого отношения к коррупции

	нове нетерпимого отношения к коррупции	рупции	рупции	коррупции	

В результате освоения дисциплины (модуля) обучающийся должен:
знать:
− особенности предмета и метода регулирования информационных правоотношений;
− характерные особенности правоотношений, складывающихся в информационной сфере, виды информационных правоотношений и основы их нормативно-правового регулирования;
− правовые режимы отдельных видов информации;
− значение информации и информационных ресурсов в современном обществе;
- основы правовых знаний в различных сферах деятельности;
уметь:
− оперировать основными понятиями и категориями информационного права;
− анализировать юридические факты, лежащие в основе возникновения,
изменения и прекращения информационных правоотношений, правильно толковать и применять нормы информационного права, принимать решения и совершать юридические действия в строгом соответствии с нормами законодательства РФ;
− грамотно составлять и оформлять юридические и служебные документы;
- использовать основы правовых знаний в различных сферах деятельности;
- определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
владеть:
− юридической терминологией, навыками работы с нормативно-правовыми
актами, регламентирующими правоотношения в информационной сфере;
− основными положениями федерального законодательства по вопросам защиты различных видов конфиденциальной информации;
− основными положениями федерального законодательства по вопросам защиты сведений, отнесенных к государственной тайне;
− основными положениями обеспечения режима секретности;
− навыками реализации норм материального и процессуального права;
− навыками обеспечения защиты государственной тайны и соблюдения режима секретности в процессе служебной деятельности
- способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

3.1 Матрица соотнесения тем/разделов учебной дисциплины и формируемых в них компетенций

Темы, разделы дисциплины	УК-2, УК-10	Σ общее количество компетенций
Раздел 1 Теоретические аспекты информационных правоотношений экономических систем		
Основные понятия курса информационное право (ИП). Виды несанкционированных атак на информацию. Современное информационное право в России. Экономическая информация как товар и объект правоотношений.	+	2
Природа возникновения угроз. Классификация угроз. Защита от несанкционированного доступа	+	2
Раздел 2 Законодательный уровень информационно-правовых отношений		
Значение законодательного уровня информационной безопас-	+	2

ности. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.		
Стандарты и спецификации в области информационной безопасности.	+	2
Раздел 3. Административный уровень информационного права		
Особенности административного уровня информационного права. Политика ИП. Управление рисками информационных правоотношений.	+	2
Процедурный уровень информационных правоотношений. Основные классы мер процедурного уровня. Управление персоналом. Реагирования на нарушения	+	2
Раздел 4. Программно-технический уровень информационной защиты		
Основные понятия правового программно-технического уровня. Архитектурная безопасность. Идентификация, аутентификация, управление доступом	+	2
Обзор биометрических технологий. Аппаратно-программные средства контроля доступа. Биометрические устройства вода. Комбинированные устройства ввода. Электронные замки	+	2
Раздел 5. Основы криптографии		
Основные понятия криптографии. Классификация шифров	+	2

4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины - 2 зачетные единицы 72 академических часов.

4.1. Объем дисциплины и виды учебной работы

Вид занятий	Количество ак. часов	
	по очной форме обучения 3 семестр	по заочной форме обучения 2 курс
Общая трудоемкость дисциплины	72	72
Контактная работа обучающихся с преподавателем	24	10
Аудиторные занятия, в т.ч.	24	10
лекции	12	4
практические занятия	12	6
Самостоятельная работа:	48	58
проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	20	30
выполнение индивидуальных заданий	15	9
подготовка к тестированию	13	9
Контроль	-	4
Вид итогового контроля	зачет	зачет

4.2. Лекции

№	Раздел дисциплины (модуля), темы лекций и их содержание	Объем в ак. часах		Формируемые компетенции
		форма обучения		
		Очная	Заочная	
1	Раздел 1.Теоретические аспекты информационной безопасности экономических систем 1.1. Основные понятия курса информационное право	1	1	УК-2, УК-10

	(ИП). Виды несанкционированных атак на информацию. Современное информационное право в России. Экономическая информация как товар и объект правоотношений			
	1.2. Природа возникновения угроз. Классификация угроз. Защита от несанкционированного доступа	1		УК-2, УК-10
2	Раздел 2. Законодательный уровень информационной безопасности 2.1. Значение законодательного уровня информационной безопасности. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности	1	1	УК-2, УК-10
	2.2 Стандарты и спецификации в области информационной безопасности	1		УК-2, УК-10
3	Раздел 3. Административный уровень информационного права 3.1. Особенности административного уровня информационного права. Политика ИП. Управление рисками информационных правоотношений.	2	1	УК-2, УК-10
	3.2. Процедурный уровень информационных правоотношений. Основные классы мер процедурного уровня. Управление персоналом. Реагирования на нарушения	2		УК-2, УК-10
4	Раздел 4. Программно-технический уровень информационной защиты 4.1. Основные понятия программно-технического уровня. Архитектурная безопасность. Идентификация, аутентификация, управление доступом	1	1	УК-2, УК-10
	4.2.Обзор биометрических технологий. Аппаратно-программные средства контроля доступа. Биометрические устройства вода. Комбинированные устройства ввода. Электронные замки	1		УК-2, УК-10
5	Раздел 5.Основы криптографии 5.1. Основные понятия криптографии. Классификация шифров	2	-	УК-2, УК-10
	Итого	12	4	

4.3. Практические занятия

№	Раздел дисциплины (модуля), темы лекций и их содержание	Объем в ак. часах		Формируемые компетенции
		форма обучения		
		Очная	Заочная	
1	Раздел 1.Теоретические аспекты информационной безопасности экономических систем 1.1. Основные понятия курса информационное право (ИП). Виды несанкционированных атак на информацию. Современное информационное право в России. Экономическая информация как товар и объект правоотношений	2	1	УК-2, УК-10
	1.2. Природа возникновения угроз. Классификация угроз. Защита от несанкционированного доступа	2		УК-2, УК-10

2	Раздел 2. Законодательный уровень информационной безопасности 2.1. Значение законодательного уровня информационной безопасности. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности	2	1	УК-2, УК-10
	2.2 Стандарты и спецификации в области информационной безопасности	1		УК-2, УК-10
3	Раздел 3. Административный уровень информационного права 3.1. Особенности административного уровня информационного права. Политика ИП. Управление рисками информационных правоотношений.	1	1	УК-2, УК-10
	3.2. Процедурный уровень информационных правоотношений. Основные классы мер процедурного уровня. Управление персоналом. Реагирования на нарушения	1		УК-2, УК-10
4	Раздел 4. Программно-технический уровень информационной защиты 4.1. Основные понятия программно-технического уровня. Архитектурная безопасность. Идентификация, аутентификация, управление доступом	1	1	УК-2, УК-10
	4.2.Обзор биометрических технологий. Аппаратно-программные средства контроля доступа. Биометрические устройства вода. Комбинированные устройства ввода. Электронные замки	1		УК-2, УК-10
5	Раздел 5.Основы криптографии 5.1. Основные понятия криптографии. Классификация шифров	1	2	УК-2, УК-10
	Итого	12	6	

4.4. Лабораторные занятия – не предусмотрены

4.5. Самостоятельная работа обучающихся

Раздел дисциплины	Вид самостоятельной работы	Объем ак. часов	
		форма обучения	
		очная	заочная
Раздел 1 Теоретические аспекты информационных правоотношений экономических систем	проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	4	6
	выполнение индивидуальных заданий	3	1
	подготовка к тестированию	3	1
Раздел 2 Законодательный уровень информационно-правовых отношений	проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	4	6
	выполнение индивидуальных заданий	3	3
	подготовка к тестированию	3	3
Раздел 3. Административный уровень информационного права	проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	4	6
	выполнение индивидуальных заданий	3	1
	подготовка к тестированию	3	1
Раздел 4. Программно-	проработка учебного материала по дисци-	4	6

технический уровень информационной защиты	плине (конспектов лекций, учебников, материалов сетевых ресурсов)		
	выполнение индивидуальных заданий	3	2
	подготовка к тестированию	2	2
Раздел 5. Основы криптографии	проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	4	6
	выполнение индивидуальных заданий	3	2
	подготовка к тестированию	2	2
Итого:		48	58

Перечень методического обеспечения для самостоятельной работы по дисциплине (модулю):

Электронный учебно-методический комплекс «Информационное право», А.Н. Грязнев, 2018 г

4.6. Выполнение контрольной работы обучающимися заочной формы

Контрольная работа состоит из 5 практических заданий, которые обучающийся выполняет согласно шифру своей зачетной книжки.

Все практические задания начинаются с изучения теоретического материала и заканчиваются оформлением отчета.

Практическое задание № 1

«Анализ рисков информационно-правовых отношений»

Цель работы. Ознакомиться с алгоритмами оценки риска информационно-правовых отношений.

Задание

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»
2. Ознакомьтесь с Приложениями С, D и Е ГОСТа.
3. Выберите три различных информационных актива организации (организация выбирается по № зачетной книжки, см. вариант).
4. Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь Приложением С ГОСТа напишите три угрозы информационно-правовых отношений, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь одним из методов (см. вариант) предложенных в Приложении Е ГОСТа произведите оценку рисков информационно-правовых отношений.
7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы информационно- правовых отношений.

Содержание отчета

1. Обоснование выбора информационных активов организации
2. Оценка ценности информационных активов
3. Уязвимости системы правовой защиты информации
4. Угрозы информационно-правовых отношений
5. Оценка рисков
6. Выводы

Вариант задания №1 – номер по двум последним цифрам в зачетной книжке обучающегося

Номер последних двух цифр зачетной книжки	Организация	Метод оценки риска (см. Приложение Е ГОСТа)
1, 31,61,91	Отделение коммерческого банка	1
2, 32,62,92	Поликлиника	2

3, 33,63,93	Колледж	3
4, 34,64,94	Офис страховой компании	4
5,35,65,95	Рекрутинговое агентство	1
6,36,66,96	Интернет-магазин	2
7,37,67,97	Центр оказания государственных услуг	3
8,38,68,98	Отделение полиции	4
9,39,69,99	Аудиторская компания	1
10,40,70	Дизайнерская фирма	2
11,41,71	Офис интернет-провайдера	3
12,42,72	Офис адвоката	4
13,43,73	Компания по разработке ПО для сторонних организаций	1
14,44,74	Агентство недвижимости	2
15,45,75	Туристическое агентство	3
16,46,76	Офис благотворительного фонда	4
17,47,77	Издательство	1
18,48,78	Консалтинговая фирма	2
19,49,79	Рекламное агентство	3
20,50,80	Отделение налоговой службы	4
21,51,81	Офис нотариуса	1
22,52,82	Бюро перевода (документов)	2
23,53,83	Научно проектное предприятие	3
24,54,84	Брачное агентство	4
25,55,85	Редакция газеты	1
26,56,86	Гостиница	2
27,57,87	Праздничное агентство	3
28,58,88	Городской архив	4
29,59,89	Диспетчерская служба такси	1
30,60,90	Железнодорожная касса	2

Практическое задание № 2.

«Информационное право в ведущих зарубежных странах»

Цель работы. Ознакомление с основными принципами информационно-правовых отношений в ведущих зарубежных странах.

Задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя учебное пособие Т.Г. Почепцов «Информационная политика» и другие доступные источники информации, в том числе ресурсы электронных библиотек
2. Заполнить таблицу " Системы информационно-правовых в ведущих зарубежных странах "(см. вариант) на основе подготовленного материала, а также докладов других обучающихся
3. Провести анализ собранной информации и сделать выводы.

Вариант – номер по двум последним шифрам в зачетной книжке.

Страна	Основные принципы ИП	Основные нормативно-правовые акты ИП	Структура государственных органов национального ИП
США	1, 28, 55,82	2,37,64,91	3,46,73
Евросоюз	4,29, 56,83	5,38,65,92	6,47,74
Великобритания	7,30, 57,84	8,39,66,93	9,48,75
Швеция	10,31, 58,85	11,40,67,94	12,49,76

Франция	13,32, 59,86	14,41,68,95	15,50,77
Германия	16,33,60,87	17,42,69,96	18,51,78
Китай	19,34, 61,88	20,43,70,97	21,52,79
Япония	22,35,62,89	23,44,71,98	24,53,80
Швейцария	25,36,63,90	26,45,72,99	27,54,81

Практическое задание № 3

«Построение концепции информационно-правовых отношений на предприятии»

Цель работы. Знакомство с основными принципами построения концепции информационно-правовых отношений на предприятии, с учетом особенностей его информационной инфраструктуры.

Задание

Разработать концепцию информационно-правовых отношений компании (см. вариант в задании №1 из Таблицы вариантов), содержащую следующие основные пункты (приведен примерный план):

1. Общие положения

Назначение Концепции информационно-правовых отношений.

1.2. Цели концепции информационно-правовых отношений

1.3. Задачи концепции информационно-правовых отношений.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационно-правовых отношений.

2.2. Определение вероятного нарушителя информационно-правовых отношений.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационно-правовых отношений предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационно-правовых отношений.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы информационно-правовых отношений на Предприятии

3.1. Принципы, условия и требования к организации и функционированию системы информационно-правовых отношений.

3.2. Основные направления политики в сфере информационно-правовых отношений.

3.3. Планирование мероприятий по регулированию информационно-правовых отношений Предприятия.

3.4. Критерии и показатели информационно-правовых отношений Предприятия.

4. Мероприятия по реализации регулирования информационно-правовых отношений на Предприятии

4.1. Организационное обеспечение выполнения требований норм информационного права.

- Задачи организационного обеспечения выполнения требований норм информационного права.
- Подразделения, занятые в обеспечении выполнения требований норм информационного права.
- Взаимодействие подразделений, занятых в обеспечении выполнения требований норм информационного права.

4.2. Техническое обеспечение выполнения требований норм информационного права на Предприятия.

- Общие положения.
- Правовая защита информационных ресурсов от несанкционированного доступа.

- Средства комплексной защиты от потенциальных угроз информационно-правовых отношений.
- Обеспечение качества информационно-правовых отношений.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия.
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационно-правовых отношений на Предприятии.

Практическое задание №4

«Программная реализация криптографических алгоритмов»

Цель работы. Правовое знакомство с основными методами криптографической зашиты информации.

Задание

Правовое изучение и применение одного из алгоритмов симметричного шифрования.

1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.
2. Выполнить проверку, расшифровав полученное сообщение.

№последних двух цифр зачетной книжки	Алгоритм шифрования
1.	Шифр Цезаря
2.	Полибианский квадрат
3.	Простая перестановка
4.	Одиночная перестановка
5.	Двойная перестановка
6.	Магический квадрат
7.	Шифр Гронсфельда
8.	Многоалфавитная замена
9.	Простая перестановка
0.	Одиночная перестановка

Вариант – по номеру последней цифры в зачетной книжке

Практическое задание № 5

«Пакеты антивирусных программ»

Цель работы. Ознакомление с основными функциями, достоинствами и недостатками современного антивирусного ПО.

Задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.
2. Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.
3. Провести анализ собранной информации и сделать выводы по следующим пунктам:

а) основные функции Антивирусной программы;

б) достоинства

в) недостатки

Вариант – номер по последней цифре в зачетной книжке:
1. Антивирус Касперского.
2. Антивирус Dr.Web для Windows
3. Panda Antivirus
4. ESET NOD32 Антивирус
5. Avast! Free Antivirus
6. Avira AntiVir Personal
7. Norton AntiVirus
8. Trend Micro Internet Security
9. Microsoft Security Essentials
0. McAfee VirusScan

4.7. Содержание разделов дисциплины

Раздел 1. Теоретические аспекты информационно-правовых отношений экономических систем

Основные понятия курса информационное право (ИП). Виды несанкционированных атак на информацию. Современное информационное право в России. Экономическая информация как товар и объект информационно-правовых отношений. Угрозы информационно-правовых отношений. Природа возникновения угроз информационно-правовых отношений. Классификация угроз. Защита от несанкционированного доступа

Раздел 2. Законодательный уровень информационной безопасности

Значение законодательного уровня информационной безопасности (ИБ). Обзор российского законодательства в области ИБ. Правовые акты общего назначения, затрагивающие вопросы ИБ. Стандарты и спецификации в области ИБ. Основные понятия. Классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800

Сетевые сервисы безопасности. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Требования доверия информации. Гармонизированные критерии Европейских стран. Интерпретация "Оранжевой книги" для сетевых конфигураций. Руководящие документы Гостехкомиссии России. Расследование компьютерных преступлений

Раздел 3. Административный уровень информационно-правовых отношений

Особенности административного уровня информационно-правовых отношений. Особенности политики информационно-правовых отношений на административном уровне. Программа развития информационно-правовых отношений на предприятиях различных уровней. Синхронизация программы развития информационно-правовых отношений с жизненным циклом систем. Процедурный уровень информационно-правовых отношений. Основные классы мер процедурного уровня. Управление персоналом для обеспечения правовой защиты информации на предприятиях различных сфер. Реагирования на нарушения.

Раздел 4.Программно-технический уровень защиты информационно-правовых отношений

Основные понятия программно-технического уровня защиты информационно-правовых отношений. Особенности архитектурной безопасности. Идентификация, аутентификация, управление доступом. Обзор биометрических технологий. Аппаратно-программные средства контроля доступа к информации на различных уровнях Биометрические устройства вода. Комбинированные устройства ввода. Электронные замки

Раздел 5. Основы криптографии

Основные понятия криптографии. Классификация шифров.

5. Образовательные технологии

При изучении дисциплины используется инновационная образовательная технология на основе интеграции компетентностного и личностно-ориентированного подходов с элементами традиционного лекционно-семинарского и квазипрофессионального обучения с использованием интерактивных форм проведения занятий, исследовательской проектной деятельности и мультимедийных учебных материалов.

Вид учебной работы	Образовательные технологии
Лекции	Электронные материалы (в т.ч. сетевые источники), использование мультимедийных средств, раздаточный материал.
Практические занятия	Тестирование, выполнение групповых аудиторных заданий, индивидуальные доклады.
Самостоятельныя работы	Выполнение реферативной работы; подготовка и защита сообщения с использованием слайдовых презентаций.

6. Оценочные средства дисциплины (модуля)

6.1. Паспорт фонда оценочных средств по дисциплине (модулю) «Информационная право»

№	Контролируемые разделы (темы) дисциплины*	Код контролируемой компетенции	Оценочное средство	
			наименование	кол-во
1	Раздел 1.Встроенные системы и сервисы защиты информации ЭВМ 1.1. Встроенная система защиты современных операционных систем	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
	1.2. Изучение средств управления встроенной системы защиты Windows	УК-2, УК-10	Вопросы к зачету	10
	1.3. Установление доступа к файлам и папкам. Оценка защищенности компьютера	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
2	Раздел 2.Нормативно-правовое обеспечение информационной безопасности 2.1. Применение российского законодательства в области ИБ для решения задач обеспечения защиты информации на разных уровнях. Правовые акты общего назначения, затрагивающие вопросы ИБ. Работа в «Консультант плюс».	УК-2, УК-10	Тестовые задания Темы рефератов	10 3
	2.2. Применение стандартов, спецификаций и других нормативно-правовых актов в области ИБ. Работа в «Консультант плюс»	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
3	Раздел 3 .Организация защиты информации в экономических системах 3.1. Анализ рисков информационно-правовых отношений	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
	3.2. Анализ развития информационно-правовых отношений в ведущих зарубежных странах	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
	3.3. Построение концепции информационно-правовых отношений на предприятия	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
4	Раздел 4. Правовые основы обеспечения защиты информации в сети Internet 4.1. Программно-аппаратные методы защиты от удаленных несанкционированных атак в сети Internet. Программные методы защиты, применяемые в сети Internet.	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
	4.2. Работа с антивирусными средствами защиты информации. Классификация антивирусных программ. Сканеры	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
	4.3. Электронная цифровая подпись и правовые	УК-2, УК-10	Вопросы к зачету	10

	особенности ее применения. Защита информации в Интернете		Темы рефератов	3
	4.4. Поиск, использование и сохранение программных продуктов. Обзор современных антивирусных программ.	УК-2, УК-10	Вопросы к зачету Темы рефератов	10 3
5	Раздел 5. Криптография и шифрование 5.1. Алгоритмы и ключи	УК-2, УК-10	Вопросы к зачету Темы рефератов	15 3
	5.2. Работа с шифрами	УК-2, УК-10	Вопросы к зачету Темы рефератов	15 3

6.2. Перечень вопросов к зачету (УК-2, УК-10)

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….
2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.
3. Правовая гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано
5. Информация, наличие которой необходимо для функционирования организаций:
6. Информация, которую трудно восстановить, однако организация может эффективно функционировать и без нее, называют:
7. Информация, которая может быть заменена или восстановлена, но процесс восстановления очень труден и связан с большими затратами, это:
8. Терминалы – это…
9. НЕСУЩЕСТВУЮЩИЕ средства защиты информации:
10. К формам защиты информации НЕ ОТНОСИТСЯ
11. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….
12. К принципам информационного права относятся
13. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…
14. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
15. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
16. Информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:
17. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:
18. Правовой уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:
19. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:
20. Особенностями информационного оружия являются:
21. К функциям информационного права относятся:
22. К типам угроз систем информационно-правовых отношений относятся

23. Хранение паролей может осуществляться
24. К тщательно контролируемым зонам относятся:
25. К национальным интересам РФ в информационной сфере относятся:
26. Информационное право это:
27. Наиболее распространенные угрозы информационно-правовых отношений:
28. Что относится к классу информационных ресурсов:
29. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:
30. Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:
31. Идентификатор субъекта доступа, который является его секретом:
32. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:
33. Правовая защита персональных данных, государственной, служебной и других видов информации ограниченного доступа это:
34. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это:
35. Реализация конституционных прав и свобод человека, обеспечение личной безопасности, повышение качества и уровня жизни это:
36. Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:
37. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы, называется:
38. Вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач, называется:
39. К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»
40. Состояние защищенности при котором не угрожает опасность это:
41. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
42. Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, правовые средства и технологии силового воздействия на информационную сферу этих государств:
43. Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности это:
44. Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы
45. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:
46. Защита от случайных и преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации это:
47. Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:

48. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:

49. Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость:

50. Гарантия того, что в любой момент времени может быть произведена полноценная проверка любого компонента программного комплекса АС:

51. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:

52. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:

53. Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом правовых общественных отношений

54. К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…»

55. Правовая защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:

56. Правовая защищенность от негативных информационно-психологических и информационно- технических воздействий:

57. Возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования информации противником это:

58. Обобщение правовых интересов личности в этой сфере, упрочнение демократии, создание правового государства это:

59. Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.

60. Правовая гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:

61. Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:

62. Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:

63. Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:

64. Действие субъектов по правовому обеспечению пользователей информационными продуктами:

65. К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики, сведения о семейном положении, сведения об имущественном или финансовом состоянии…»

66. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:

67. Действия, предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:

68. Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

69. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и никто другой:

70. Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

71. Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:

72. Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:

73. К какому уровню доступа информации относится следующая информация: «Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия…»

74. Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые

75. Использование основ правовых знаний в профессиональной деятельности заключается в …

76. Задачи по обеспечению информационно-правовых отношений для разных категорий субъектов могут:

77. Вопросы правоотношений распределенных систем регулируются нормативным актом получившим название –

78. Аутентификация – это сервис обеспечивающий:

79. Аутентификация партнеров по общению используется при:

80. Управление доступом обеспечивает:

81. Конфиденциальность данных обеспечивает:

82. Отдельно выделяется конфиденциальность трафика – это защита информации, которую можно получить:

83. Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг:

84. Администрирование информационной системы в целом включает (три пункта):

85. Администрирование сервисов безопасности включает в себя (три пункта):

86. В состав автоматизированной информационной системы входят следующие компоненты:

87. Аппаратные средства – это:

88. Программное обеспечение – это (несколько):

89. Данные – это:

90. Персонал – это

91. Специалист по информационной безопасности (начальник службы безопасности, администратор по безопасности) играет:

92. Владелец информации – лицо,

93. Поставщики аппаратного и программного обеспечения обычно являются сторонними лицами, которые:

94. Администратор сети – лицо, занимающееся (отметьте несколько):

95. Менеджер отдела должен (выберите несколько):

96. Операторы на предприятиях должны:

97. Аудиторы – внешние специалисты по безопасности, нанимаемые организацией для:

98. Причинами случайных воздействий при эксплуатации могут быть (отметьте лишнее):

99. Преднамеренные воздействия – это:

100. Действия нарушителя могут быть обусловлены разными мотивами, это:

101. Угрозы информационно-правовых отношений, классифицируемые по расположению источника угроз, бывают (укажите лишнее:

102. Каналы несанкционированного доступа классифицируются по компонентам автоматизированных информационных систем (укажите лишнее):

103. Компьютерный вирус — разновидность компьютерных программ, отличительной особенностью которой является:

104. Вирусы могут:
105. По среде "обитания" вирусы делятся на (отметьте лишнее):
106. По особенностям алгоритма работы вирусы делятся на (укажите лишнее):
107. Какие законы существуют в России в области компьютерного права? (выберете несколько вариантов)
108. Какие существуют основные уровни обеспечения правовой защиты информации? (несколько вариантов)
109. Физические средства защиты информации:
110. В чем заключается основная причина потерь информации, связанной с ПК?
111. Технические средства защиты информации:
112. К аспектам ИП относятся: (несколько вариантов)
113. Что такое криптология?
114. Что такое несанкционированный доступ (нсд)?
115. Что такое целостность информации?
116. В чем состоит задача криптографа?
117. Под информационным правом понимают:
118. Что такое аутентификация?
119. Утечка информации – это:
120. Под изоляцией и разделением (требование к обеспечению ИБ) понимают:
121. Уровень секретности – это:
122. Угроза – это:
123. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации, называется:
124. Организационные угрозы подразделяются на (несколько вариантов):
125. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется:
126. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?
127. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется:
128. К методам защиты от несанкционированного доступа информации относятся (несколько вариантов):
129. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется (несколько вариантов):
130. Что такое компьютерный вирус?
131. Информационные технологии (в соответствии с законом) – это:
132. Обладатель информации (в соответствии с законом) – это:
133. Доступ к информации (в соответствии с законом) – это:
134. Конфиденциальность информации (в соответствии с законом) - это:
135. Предоставление информации (в соответствии с законом) – это:
136. Распространение информации (в соответствии с законом) – это:
137. Электронное сообщение (в соответствии с законом) – это:
138. Документированная информация (в соответствии с законом) – это:
139. Электронный документ (в соответствии с законом) – это:
140. Оператор информационной системы (в соответствии с законом) – это:
141. Информация в зависимости от категории доступа подразделяется (в соответствии с законом) на:
142. Защита информации осуществляется путем применения мер:
143. Государственная тайна - защищаемые государством сведения в области его:
144. Информационные характеристики системы классификации АС, включают в себя:

145. Какой из перечисленных документов излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа:

146. Несанкционированный доступ определяется, как:

147. Информация как объект правовых отношений, может являться объектом (в соответствии с законом):

148. Информация в зависимости от порядка ее предоставления или распространения (в соответствии с законом) подразделяется на (отметьте лишнее):

149. Обладателем информации (в соответствии с законом) может быть (укажите лишний вариант):

150. Преобразовательный процесс, при котором исходный (открытый) текст заменяется шифрованным текстом, носит название:

6.3. Шкала оценочных средств

Уровни сформированности компетенций	Критерии оценивания	Оценочные средства (кол-во баллов)
Продвинутый (75 -100 баллов) «зачтено»	Знает. Успешное и систематическое применение знаний о системе различных информационных ресурсов и технологий, основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации; инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации, и способов обоснования своего выбора Умеет. Сформированное умение работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации; системы инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации; использовать основы правовых знаний в различных сферах деятельности. Владеет. Успешные и систематические навыки сбора, обработки, систематизации и анализа информации; Успешное и систематическое владение навыками выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	тестовые задания (32-40 баллов); реферат (5-10 баллов); вопросы к зачету (38-50 баллов)
Базовый (50 -74 балла) «зачтено»	Знает. Сформированные, но содержащие отдельные пробелы знания системы различных информационных ресурсов и технологий, основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации; содержания и структуры инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации, и способов обоснования своего выбора Умеет. В целом успешное, но содержащее отдельные пробелы в применении основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации; системы инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации Владеет. В целом успешные, но содержащие отдельные пробелы навыки сбора, обработки, систематизации и анализа информации; навыками выбора инструментальных средств для обработки фи-	тестовые задания (22-32 баллов); реферат (3-6 баллов); вопросы к зачету (25-36 баллов)

	нансовой, бухгалтерской и иной экономической информации	
Пороговый (35 - 49 баллов) «зачтено»	Знает. Общие, но не структурированные знания системы различных информационных ресурсов и технологий, основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации; содержания и структуры инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации, и способов обоснования своего выбора Умеет. В целом успешное, но не систематическое применение основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации; системы инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации Владеет. В целом успешное, но не систематическое владение навыками сбора, обработки, систематизации и анализа информации; навыками выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	тестовые задания (15-20 баллов); реферат (2-6 балла); вопросы к зачету (18-23 баллов)
Низкий (допороговый) (компетенция не сформирована) (0-34 балла) – «не зачтено»	Знает. Фрагментарные знания системы различных информационных ресурсов и технологий, основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации; содержания и структуры инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и способов обоснования своего выбора Умеет. Частично освоенное умение работать с различными информационными ресурсами и технологиями; системой инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации Владеет. Фрагментарное применение навыков сбора, обработки, систематизации и анализа информации; навыками выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	тестовые задания (0-14 баллов); реферат (0-5 балл); вопросы к зачету (0-15 баллов)

Все комплекты оценочных средств (контрольно-измерительных материалов), необходимых для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения дисциплины (модуля) подробно представлены в документе «Фонд оценочных средств дисциплины (модуля)».

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная учебная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8.

https://www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847— Загл. с экрана

2. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. https://www.biblio-

online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1— Загл. с экрана

3. Информационные технологии: учебное пособие / Ю.Ю. Громов, В.Е. Дидрих, И.В. Дидрих, Ю.Ф. Мартемьянов, В.О. Драчев, В.Г. Однолько. [Электронный ресурс] — Электрон. дан. – Тамбов: Изд-во ГОУ ВПО ТГТУ, 2011. – 152 с. – 100 экз. – ISBN 978-5-8265-0993-7. — Режим доступа: http://ebs.rgazu.ru/?q=node/545 — Загл. с экрана

7.2.Дополнительная учебная литература:

Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4.https://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7

7.3Методические указания по освоению дисциплины

Электронный учебно-методический комплекс «Информационное право», А.Н. Грязнев, 2023 г.

7.4 Информационные и цифровые технологии (программное обеспечение, современные профессиональные базы данных и информационные справочные системы)

Учебная дисциплина (модуль) предусматривает освоение информационных и цифровых технологий. Реализация цифровых технологий в образовательном пространстве является одной из важнейших целей образования, дающей возможность развивать конкурентоспособные качества обучающихся как будущих высококвалифицированных специалистов.

Цифровые технологии предусматривают развитие навыков эффективного решения задач профессионального, социального, личностного характера с использованием различных видов коммуникационных технологий. Освоение цифровых технологий в рамках данной дисциплины (модуля) ориентировано на способность безопасно и надлежащим образом получать доступ, управлять, интегрировать, обмениваться, оценивать и создавать информацию с помощью цифровых устройств и сетевых технологий. Формирование цифровой компетентности предполагает работу с данными, владение инструментами для коммуникации.

7.4.1 Электронно-библиотечные системы и базы данных

1. ООО «ЭБС ЛАНЬ» (https://e.lanbook.ru/) (договор на оказание услуг от 03.04.2024 № б/н (Сетевая электронная библиотека)

2. База данных электронных информационных ресурсов ФГБНУ ЦНСХБ (договор по обеспечению доступа к электронным информационным ресурсам ФГБНУ ЦНСХБ через терминал удаленного доступа (ТУД ФГБНУ ЦНСХБ) от 09.04.2024 № 05-УТ/2024)

3. Электронная библиотечная система «Национальный цифровой ресурс «Руконт»: Коллекции «Базовый массив» и «Колос-с. Сельское хозяйство» (https://rucont.ru/) (договор на оказание услуг по предоставлению доступа от 26.04.2024 № 1901/БП22)

4. ООО «Электронное издательство ЮРАЙТ» (https://urait.ru/) (договор на оказание услуг по предоставлению доступа к образовательной платформе ООО «Электронное издательство ЮРАЙТ» от 07.05.2024 № 6555)

5. Электронно-библиотечная система «Вернадский» (https://vernadsky-lib.ru) (договор на безвозмездное использование произведений от 26.03.2020 № 14/20/25)

6. База данных НЭБ «Национальная электронная библиотека» (https://rusneb.ru/) (договор о подключении к НЭБ и предоставлении доступа к объектам НЭБ от 01.08.2018 № 101/НЭБ/4712)

7. Соглашение о сотрудничестве по оказанию библиотечно-информационных и социокультурных услуг пользователям университета из числа инвалидов по зрению, слабовидящих, инвалидов других категорий с ограниченным доступом к информации, лиц, имеющих трудности с чтением плоскопечатного текста ТОГБУК «Тамбовская областная универсальная научная библиотека им. А.С. Пушкина» (https://www.tambovlib.ru) (соглашение о сотрудничестве от 16.09.2021 № б/н)

7.4.2. Информационные справочные системы

1. Справочная правовая система КонсультантПлюс (договор поставки, адаптации и сопровождения экземпляров систем КонсультантПлюс от 11.03.2024 № 11921 /13900/ЭС)

2. Электронный периодический справочник «Система ГАРАНТ» (договор на услуги по сопровождению от 15.01.2024 № 194-01/2024)

7.4.3. Современные профессиональные базы данных

1. База данных нормативно-правовых актов информационно-образовательной программы «Росметод» (договор от 15.08.2023 № 542/2023)

2. База данных Научной электронной библиотеки eLIBRARY.RU – российский информационно-аналитический портал в области науки, технологии, медицины и образования - https://elibrary.ru/

3. Портал открытых данных Российской Федерации - https://data.gov.ru/

4. Открытые данные Федеральной службы государственной статистики - https://rosstat.gov.ru/opendataПрофессиональные базы данных. Защита информации http://www.iso27000.ru/

5. Профессиональные базы данных. Международный научно-образовательный сайт EqWorld http://eqworld.ipmnet.ru/indexr.htm

6.Профессиональные базы данных. им. Е.И. Овсянкина. Информационная безопасность. Защита информации http://all-ib.ru/

7.4.4. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

№	Наименование	Разработчик ПО (правообладатель)	Доступность (лицензионное, свободно распространяемое)	Ссылка на Единый реестр российских программ для ЭВМ и БД (при наличии)	Реквизиты подтверждающего документа (при наличии)
1	Microsoft Windows, Office Professional	Microsoft Corporation	Лицензионное	-	Лицензия от 04.06.2015 № 65291651 срок действия: бессрочно
2	Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса	АО «Лаборатория Касперского» (Россия)	Лицензионное	https://reestr.digital.gov.ru/reestr/366574/?sphrase_id=415165	Сублицензионный договор с ООО «Софтекс» от 24.10.2023 № б/н, срок действия: с 22.11.2023 по 22.11.2024
3	МойОфис Стандартный - Офисный пакет для работы с документами и почтой (myoffice.ru)	ООО «Новые облачные технологии» (Россия)	Лицензионное	https://reestr.digital.gov.ru/reestr/301631/?sphrase_id=2698444	Контракт с ООО «Рубикон» от 24.04.2019 № 0364100000819000012 срок действия: бессрочно
4	Офисный пакет «Р7-Офис» (десктопная вер-	АО «Р7»	Лицензионное	https://reestr.digital.gov.ru/reestr/306668/?sphrase_id=4435041	Контракт с ООО «Софтекс»

	сия)				от 24.10.2023 № 03641000008230 00007 срок действия: бессрочно
5	Операционная система «Альт Образование»	ООО "Базальт свободное программное обеспечение"	Лицензионное	https://reestr.digital.gov.ru/reestr/303262/?sphrase_id=4435015	Контракт с ООО «Софтекс» от 24.10.2023 № 03641000008230 00007 срок действия: бессрочно
6	Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат ВУЗ» (https://docs.antiplagiaus.ru)	АО «Антиплагиат» (Россия)	Лицензионное	https://reestr.digital.gov.ru/reestr/303350/?sphrase_id=2698186	Лицензионный договор с АО «Антиплагиат» от 23.05.2024 № 8151, срок действия: с 23.05.2024 по 22.05.2025
7	Acrobat Reader - просмотр документов PDF, DjVU	Adobe Systems	Свободно распространяемое	-	-
8	Foxit Reader - просмотр документов PDF, DjVU	Foxit Corporation	Свободно распространяемое	-	-

7.4.5. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. CDTOwiki: база знаний по цифровой трансформации https://cdto.wiki/
2. База тестов для текущей, рубежной и итоговой аттестации обучающихся: программный комплекс «АСТ-Тест Plus» (лицензионный договор №Л-21/16 от 18.10.2016 г.)
3. DreamSpark Premium (подписка на программные продукты Microsoft)
4. ГИС MapInfo Professional 15.0 для Windows для учебных заведений

7.4.6. Цифровые инструменты, применяемые в образовательном процессе

1. LMS-платформа Moodle
2. Виртуальная доска SBoard https://sboard.online
3. Облачные сервисы: Яндекс.Диск, Облако Mail.ru
4. Сервисы опросов: Яндекс Формы, MyQuiz

7.4.7. Цифровые технологии, применяемые при изучении дисциплины

№	Цифровые технологии	Виды учебной работы, выполняемые с применением цифровой технологии	Формируемые компетенции
1.	Облачные технологии	Лекции Практические занятия	УК-2
2.	Большие данные	Лекции Практические занятия	УК-2

3.	Технологии беспроводной связи	Лекции Практические занятия	УК-2

8. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий лекционного типа (г. Мичуринск, ул. Интернациональная, д.101 - 3/301)	Проектор Acer XD 1760D (инв. № 1101045115); 2. Экран на штативе (инв. № 1101047182); 3. Ноутбук Lenovo G570 15,6' (инв. № 410113400037); 4. Наборы демонстрационного оборудования и учебно-наглядных пособий.	1. Microsoft Windows 7 (лицензия от 31.12.2013 № 49413124, бессрочно). 2. Microsoft Office 2010 (лицензия от 04.06.2015 № 65291658, бессрочно).
Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (г. Мичуринск, ул. Интернациональная, д. 101 – 2/50)	1. Ноутбук (инв. № 1101047129) 2. Проектор Acer X113H (инв. № 21013400641) 3. Экран на штативе Lumien Eco View с возможностью настенного крепления (инв. № 21013400642).	1. Microsoft Windows 7 (лицензия от 31.12.2013 № 49413124, бессрочно). 2. Microsoft Office 2010 (лицензия от 04.06.2015 № 65291658, бессрочно). 3. Система Консультант Плюс, договор от 10.03.2017 № 7844/13900/ЭС; Система Консультант Плюс, договор от 20.02.2018 № 9012 /13900/ЭС; Система Консультант Плюс, договор от 01.11.2018 № 9447/13900/ЭС; Система Консультант Плюс, договор от 26.02.2019 № 9662/1390. 4. Электронный периодический справочник «Система ГАРАНТ», договор от 27.12.2016 № 154-01/17; Электронный периодический справочник «Система ГАРАНТ», договор от 09.01.2018 № 194-01/2018СД; Электронный периодический справочник «Система ГАРАНТ», договор от 02.07.2018 № 194-02/2018СД; Электронный периодический справочник 5. Программное обеспечение «Антиплагиат. ВУЗ» (лицензионный договор от 21.03.2018 №193, бессрочно; лицензионный договор от 10.05.2018 №193-1, бессрочно).. 6. Информационно-образовательная программа «Росметод» (договор от 17.07.2018 № 2135).
Помещение для самостоятельной работы (г. Мичуринск, ул. Интернациональная, д.101 - 1/210)	1. Шкаф канцелярский (инв. № 2101062853, 2101062852) 2. Холодильник Стинол (инв. № 2101040880) 3. Принтер HP-1100 (инв. № 2101041634) 4. Принтер HP Laser Jet 1200 (инв. №1101047381) 5. Принтер Canon (инв. № 2101045032) 6. МФУ Canon i-Sensys MF 4410 (инв. № 41013400760) 7. Системный комплект: Процессор Intel Original LGA 1155 Celeron G 1610 OEM (2.6/2 Mb), монитор 20" Asus As MS202D, материнская плата Asus, вентилятор, память, жесткий диск, корпус, клавиатура, мышь (инв. № 21013400429) 8. Ноутбук Hewlett Packard Pavilion 15-e006sr (D9X28EA) (инв. №21013400617) 9. Доска классная+маркер (инв. № 1101063872) 10. Компьютер (инв. №41013401070) 11. Компьютер (инв. №41013401082) 12. Компьютер Celeron E 3300 (инв. № 2101045217, 1101047398) 13. Компьютер Dual Core (инв. № 2101045268)	1. Microsoft Windows 7 (лицензия от 31.12.2013 № 49413124, бессрочно). 2. Microsoft Office 2010 (лицензия от 04.06.2015 № 65291658, бессрочно). 3. Система Консультант Плюс, договор от 10.03.2017 № 7844/13900/ЭС; Система Консультант Плюс, договор от 20.02.2018 № 9012 /13900/ЭС; Система Консультант Плюс, договор от 01.11.2018 № 9447/13900/ЭС; Система Консультант Плюс, договор от 26.02.2019 № 9662/13900/ЭС. 4. Электронный периодический справочник «Система ГАРАНТ», договор от 27.12.2016 № 154-01/17; Электронный периодический справочник «Система ГАРАНТ», договор от 09.01.2018 № 194-01/2018СД; Электронный периодический справочник «Система ГАРАНТ», договор от 02.07.2018 № 194-02/2018СД. 5. Программное обеспечение «Антиплаги-

	14. Компьютер OLDI 310 КД (инв. № 2101045044) 15. Копировальный аппарат Kyocera Mita TASKalfa 180 (инв. № 21013400369) Компьютерная техника подключена в сети «Интернет» и обеспечена доступом к ЭИОС университета.	ат. ВУЗ» (лицензионный договор от 21.03.2018 №193, бессрочно; лицензионный договор от 10.05.2018 №193-1, бессрочно).

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО – бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденного приказом Минобрнауки РФ от 19.09.2017г., №929.

Автор: А.Н. Грязнев преподаватель кафедры экономической безопасности и права
Рецензент(ы): Аникьева Э.Н. старший преподаватель кафедры математики, физики и информационных технологий

Рабочая программа разработана в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры правового обеспечения . Протокол № 7 от «10» апреля 2019 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 9 от 22 апреля 2019 г.

Программа утверждена Решением учебно-методического совета университета протокол №8 от 25 апреля 2019 года.

Рабочая программа переработана в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры кафедры экономической безопасности и права № 10 от «17» апреля 2020 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 9 от 13 апреля 2020 г.

Программа утверждена Решением учебно-методического совета университета протокол №8 от 23 апреля 2020 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры экономической безопасности и права. Протокол № 9 от «19» апреля 2021 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 9 от 05 апреля 2021 г.

Программа утверждена Решением учебно-методического совета университета протокол №8 от 22 апреля 2021 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры экономической безопасности и права. Протокол № 11 от «21» июня 2021 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 11 от 15 июня 2021 г.

Программа утверждена Решением учебно-методического совета университета протокол №12 от 29 июня 2021 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры экономической безопасности и права. Протокол № 9 от «13» апреля 2022 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 7 от 14 апреля 2022 г.

Программа утверждена Решением учебно-методического совета университета протокол №8 от 21 апреля 2022 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры экономической безопасности. Протокол № 11 от «09» июня 2023 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 10 от 19 июня 2023 г.

Программа утверждена Решением учебно-методического совета университета протокол №10 от 22 июня 2023 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры экономической безопасности. Протокол № 11 от «06» мая 2024 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 09 от 20 мая 2024 г.

Программа утверждена Решением учебно-методического совета университета протокол №09 от 23 мая 2024 года.

Оригинал документа хранится на кафедре математики, физики и информационных технологий