МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программа специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Организационное и правовое обеспечение информационной безопасности

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Организационное и правовое обеспечение информационной безопасности» является формирование компетенций для научно-исследовательского, организационно-управленческого видов деятельности и профессиональной специализации в области правовых и организационных вопросов обеспечения безопасности компьютерных систем. Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности). научно-исследовательская деятельность : сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности; изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте; организационно-управленческая деятельность: осуществление правового, организационного и технического обеспечения защиты информации; организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации); специализация №8 "Информационная безопасность объектов информатизации на базе компьютерных систем": разработка проектов нормативных правовых актов, руководящих и методических документов предприятия, учреждения, регламентирующих деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ПК-1 - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах;

ПК-9 - Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию;

ПК-10 - Способен организовать процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПК-25 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-28 - Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

Понимает значение информации и информационной безопасности в развитии современного общества, значимость своей будущей профессии.

Уметь:

Использует нормативные правовые акты и нормативные методические документы, регламентирующие деятельность по информационной безопасности, в своей профессиональной деятельности.

Уметь:

Использует нормативные правовые акты и нормативные методические документы, регламентирующие деятельность по разработке и сопровождению современных компьютерных систем, в своей профессиональной деятельности.

Владеть:

Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.

Уметь:

Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.

Знать:

Участвует в проведении экспериментально-исследовательских работ при сертификации средств защиты информации.

Владеть:

Проверяет уровень квалификации, распределяет полномочия и контролирует выполнение инструкций в отношении персонала обслуживающего технические, программные и программно-аппаратные средства защиты информации.

Уметь:

Анализирует компьютерные системы в сфере профессиональной деятельности с целью выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа.

Знать:

Знать основные процессы проектирования систем обеспечения информационной безопасности.

Уметь:

Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.

Знать:

Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации.

Уметь:

Уметь разрабатывать нормативно правовые акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования.

Владеть:

Владеть навыками разработки нормативной правовой документации.

Уметь:

Разрабатывает и организует выполнение мероприятий в соответствии с положениями политики информационной безопасности и защиты информации ограниченного доступа.

Уметь:

Разрабатывает предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.

Уметь:

Формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач.

Уметь:

Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничении?.

Уметь:

Решает конкретные задачи проекта заявленного качества и за установленное время.

Уметь:

Публично представляет результаты решения конкретной задачи проекта.

Уметь:

Демонстрирует уважительное отношение к праву и закону, достаточный уровень профессионального правосознания и правовой культуры для исполнения профессиональных обязанностей, обеспечивать защиту прав интеллектуальной собственности.

Владеть:

Способен разрабатывать варианты управленческих решений в сфере профессиональной деятельности, определять обоснованность их выбора на основе критериев соответствия требованиям нормативных правовых актов.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №6
Контактная работа при проведении учебных занятий (всего):	68	68
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа	34	34

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 76 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Способен разрабатывать варианты управленческих решений в сфере профессиональной деятельности, определять обоснованность их выбора на основе критериев соответствия требованиям нормативных правовых актов.
2	Информация как объект юридической защиты.
3	Формирование государственной системы правового обеспечения информационной безопасности.
4	Правовое обеспечение защиты государственной тайны.

№ п/п	Тематика лекционных занятий / краткое содержание
5	Законодательство Российской Федерации в области информационной безопасности. Содержание информационной деятельности. Основные законодательные акты регламентирующие информационную деятельность.
6	Защита прав личности в информационной сфере.
7	Правовая защита информация в сфере высоких технологий.
8	Правовая защита интеллектуальной собственности.
9	Правовое обеспечение защиты коммерческой тайны.
10	Правовое регулирование деятельности организаций в сфере информационной безопасности.
11	Юридическая ответственность за правонарушения в области информационной безопасности.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ1 Правовое обеспечение информационной безопасности в системе информационного права.
2	ПЗ2 Информация как объект юридической защиты.
3	ПЗ3 Формирование государственной системы правового обеспечения информационной безопасности.
4	ПЗ4 Правовое обеспечение защиты государственной тайны.
5	ПЗ5 Законодательство Российской Федерации в области информационной безопасности.
6	ПЗ6 Защита прав личности в информационной сфере.
7	ПЗ7 Правовая защита информация в сфере высоких технологий.
8	ПЗ8 Правовая защита интеллектуальной собственности.
9	ПЗ9 Правовое обеспечение защиты коммерческой тайны.
10	ПЗ10 Правовое регулирование деятельности организаций в сфере информационной безопасности.
11	ПЗ11 Юридическая ответственность за правонарушения в области информационной безопасности.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Органы защиты информации. Перечень, права и обязанности органов защиты информации.
2	СР2 Защита результатов интеллектуальной деятельности. Законодательное регулирование обеспечения защиты интеллектуальных прав.
3	СР3 Лицензирование и сертификация в области защиты информации. Законодательный порядок лицензирования систем защиты информации.
4	СР4 Ответственность за компьютерные преступления. Уголовное законодательство о защите информации. Составы преступлений в области компьютерной безопасности.
5	СР5 Сущность информации и ее ресурсов. Понятие информации, информация в праве и законодательстве.
6	СР6 Информационное право как отрасль права. Регламентация информационной деятельности.
7	СР7 Юридическая ответственность в информационной сфере. Ответственность в информационных правоотношениях.
8	СР8 Конституционные гарантии неприкосновенности частной жизни, охраны личной и семейной тайны. Право на охрану личной и семейной тайны. Виды профессиональных тайн. Персональные данные
9	СР9 Правовое регулирование института государственной тайны. Государственная тайна. Сущность, роль и значение. Объекты государственной тайны.
10	СР10 Правовой режим коммерческой тайны. Коммерческая тайна. Информация, входящая в коммерческую тайну.
11	СР11 Иные виды конфиденциальной информации. Информация ограниченного доступа.
12	Подготовка к промежуточной аттестации.
13	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Основы правового обеспечения защиты информации Сёмкин С.Н., Сёмкин А.Н. Орел: Академия Спецсвязи России , 2004	
2	Организационно-правовое обеспечение информационной безопасности Стрельцов А.А., Горбатов В.С., Полякова Т.А. Академия , 2008	

3	Организационно-правовое и методическое обеспечение Кармановский Н.С., Михайличенко О.В., Савков С.В НИУ ИТМО , 2013	
1	Правовое обеспечение информационной безопасности Терехов А.В., Бурцева Е.В. Издательство ТГТУ , 2010	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Гарант – Законодательство [электронный ресурс] URL: http://www.garant.ru/ Телекоммуникационное право [электронный ресурс] URL: http://www.telecomlaw.ru «Консультант-плюс» [электронный ресурс] URL: http://www.consultant.ru/ ФСТЭК России [электронный ресурс] URL: https://fstec.ru/ ФСБ России [электронный ресурс] URL: http://www.fsb.ru/

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Для проведения практических занятий

на компьютерах должно быть установлено следующее программное обеспечение: – операционная система Microsoft Windows 7 / 8.1 / 10 (любая); – браузер Microsoft IE, Edge, Google Chrome, Mozilla Firefox (любой); – средство защиты от вредоносных программ (любое). Компьютеры должны иметь доступ в сеть «Интернет».

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения лекционных занятийнеобходима лекционная аудитория с проектором. Для проведения практических занятийжелательна аудитория с проектором и компьютерами, имеющими выход в сеть «Интернет». Требование к компьютерам: – персональный компьютер с конфигурацией не ниже Intel / 2 ядра / 2GB RAM / 80GB HDD / 1366x768 LCD.

9. Форма промежуточной аттестации:

Экзамен в 6 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, к.н. кафедры «Управление и защита информации» А.А. Привалов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин