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 - программы бакалавриата
по направлению подготовки
40.03.01 Юриспруденция,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Организационно-правовое обеспечение информационной безопасности

Направление подготовки: 40.03.01 Юриспруденция

Направленность (профиль): Юриспруденция в цифровой экономике и государственном управлении

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: 626395
Подписал: заведующий кафедрой Чеботарева Анна Александровна
Дата: 25.05.2022

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины является:

-формирование компетенций, необходимых обучающемуся для исполнения обязанностей по предстоящему должностному предназначению выбранного направления и задачам профессиональной деятельности.

Задачами дисциплины являются:

- овладение методологией получения юридически значимой информации из различных источников, включая правовые базы данных, решения задач профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности;;

- формирование навыков работы с информацией в цифровой среде, взаимодействовия в ней с учетом норм правового регулирования цифрового пространства

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-8 - Способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности ;

ПК-16 - Способен работать с информацией в цифровой среде, взаимодействовать в ней с учетом норм правового регулирования цифрового пространства.

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

Знать:

Теоретические основы-категориально-терминологический аппарат в области правового обеспечения информационной безопасности, основы противодействия информационным правонарушениям.

Уметь:

Решать задачи профессиональной деятельности с применением информационных технологий, работать с информацией в цифровой среде, взаимодействовать в ней с учетом норм правового регулирования цифрового пространства

Владеть:

Навыками решения задач профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности, а также работы с информацией в цифровой среде, взаимодействовия в ней с учетом норм правового регулирования цифрового пространства

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 1
Контактная работа при проведении учебных занятий (всего):	66	66
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	50	50

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 78 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	Понятие и правовые основы информационной безопасности. Рассматриваемые вопросы: - Подходы к опредедению понятия «информационная безопасность». - Место ИБ в системе обеспечения национальной безопасности. Национальные интересы РФ в информационной сфере. - Значение обеспечения информационной безопасности личности, общества и государства. Конституционно-правовые основы. - Принципы, задачи, функции и стандарты обеспечения информационной безопасности. - Законодательство в сфере обеспечения информационной безопасности и его место в системе российского законодательства. - Значение Доктрины информационной безопасности Российской Федерации
2	Организационные основы системы обеспечения информационной безопасности Рассматриваемые вопросы: - Основные элементы организационной основы системы обеспечения информационной безопасности - Основные задачи государственной информационной политики - Органы государственной власти – силы обеспечения информационной безопасности РФ
3	Правовые основы защиты персональных данных. Рассматриваемые вопросы: - Понятие персональных данных. Виды персональных данных - Федеральный закон «О персональных данных». - Роскомнадзор и его полномочия.
4	Значение правового обеспечения информационной безопасности в условиях развития цифровой экономики и сквозных цифровых технологий Рассматриваемые вопросы: - Реализация национальнйо программы »Цифровая экономика» и значение обеспечения информационной безопасности - Значение информационной безопасности в условиях внедрения информационных технологий на транспорте
5	Значение и правовое обеспечение государственной тайны Рассматриваемые вопросы: - Определение понятия «государственная тайна». - Перечень сведений, составляющих государственную тайну. - Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей. Порядок установления степеней секретности. Распоряжение сведениями, составляющими государственную тайну. - Правовые механизмы допуска и доступа к сведениям, составляющим государственную тайну. - Система защиты государственной тайны. - Контроль и надзор за обеспечением защиты государственной тайны. Особенности правовой защиты сведений, составляющих государственную тайну.
6	Понятие и значение безопасности критической информационной инфраструктуры Рассматриваемые вопросы: - Правовые основы безопасности критической информационной инфраструктуры. - Значение федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ - Значение информационной безопасности и безопасности критической информационной инфраструктуры на транспорте.
7	Значение международной информационной безопасности. Международный опыт борьбы с преступлениями в сфере компьютерной информации. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Основы государственной политики РФ в области международной информационной безопасности. -Международный опыт борьбы с преступлениями в сфере компьютерной информации - Опыт борьбы с преступлениями в сфере компьютеной информации в зарубежных странах
8	Информационные правонарушения и преступления в информационной сфере - Понятие и характеристика информационного правонарушения - Гражданско-правовая ответственность за информационные правонарушения. - Административно-правовая ответственность за информационные правонарушения. - Уголовная ответственность за преступления в информационной сфере. Ответственность за преступления в сфере компьютерной информации. - Криминалистическая характеристика преступлений в сфере компьютерной информации.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Понятие и правовые основы информационной безопасности Рассматриваемые вопросы: - Подходы к опредедению понятия «информационная безопасность». - Место ИБ в системе обеспечения национальной безопасности. Национальные интересы РФ в информационной сфере. - Значение обеспечения информационной безопасности личности, общества и государства. Конституционно-правовые основы. - Принципы, задачи, функции и стандарты обеспечения информационной безопасности
2	Понятие и правовые основы информационной безопасности Рассматриваемые вопросы: - Законодательство в сфере обеспечения информационной безопасности и его место в системе российского законодательства. - Значение Доктрины информационной безопасности Российской Федерации
3	Организационные основы системы обеспечения информационной безопасности Рассматриваемые вопросы: - Основные элементы организационной основы системы обеспечения информационной безопасности - Основные задачи государственной информационной политики - Органы государственной власти – силы обеспечения информационной безопасности РФ
4	Правовые основы защиты персональных данных. Рассматриваемые вопросы: - Понятие персональных данных. Виды персональных данных - Федеральный закон «О персональных данных». - Риски утечек данных. Вопросы противодействия. - Роскомнадзор и его полномочия.
5	Правовые основы защиты персональных данных. Рассматриваемые вопросы: - Связь проблемы защиты персональных данных с развитием автоматизированных систем обработки и хранения информации. Основные положения Конвенции о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.).
6	Проблемы обеспечения информационной безопасности в условиях развития электронного документооборота Рассматриваемые вопросы: - Развитие электронного документооборота. Статус электронного документа. –

№ п/п	Тематика практических занятий/краткое содержание
	- сущность электронной подписи. Проблемы правоприменения. - Особенности применения систем электронного документооборота - . Преимущества и недостатки электронного документооборота. - Значение межведомственного документооборота. Проблемы обеспечения информационной безопасности.
7	Значение института служебной тайны для защиты информации на современном этапе. Рассматриваемые вопросы: - Эволюция института служебной тайны в отечественном законодательстве - Сферы применения института служебной тайны. - Нормативное регулирования института служебной тайны. - Формирование норм ответственности за разглашение сведений, составляющих служебную тайну.
8	Институт коммерческой тайны как система защиты коммерческой информации и объектов интеллектуальной собственности. Рассматриваемые вопросы: - Цели правового регулирования информационных правоотношений при работе с информацией, составляющей коммерческую тайну. - Основные категории института коммерческой тайны (информация, составляющая коммерческую тайну, режим коммерческой тайны, носители коммерческой тайны, разглашение коммерческой тайны, неправомерные способы получения коммерческой тайны).
9	Значение правового обеспечения информационной безопасности в условиях развития цифровой экономики и сквозных цифровых технологий Рассматриваемые вопросы: - Реализация национальнйо программы «Цифровая экономика» и значение обеспечения информационной безопасности - Значение информационной безопасности в условиях внедрения информационных технологий на транспорте.
10	Значение правового обеспечения информационной безопасности в условиях развития цифровой экономики и сквозных цифровых технологий Рассматриваемые вопросы: - Развитие искусственного интеллекта и проблемы обеспечения информационной безопасности - Большие данные, риски и обеспечение информационной безопасности
11	Значение правового обеспечения информационной безопасности в условиях развития цифровой экономики и сквозных цифровых технологий Рассматриваемые вопросы: - Перспективы и проблемы внедрения технологии блокчейн. Проблемы обеспечения информационной безопасности - Особенности применения смарт-контрактов и проблемы обеспечения информационной безопасности
12	Значение правового обеспечения информационной безопасности в условиях развития цифровой экономики и сквозных цифровых технологий Рассматриваемые вопросы: - Цифровые валюты: особенности правового регулирования и проблемы обеспечения информационной безопасности - Концепция цифрового рубля и проблемы обеспечения информационной безопасности - Криптовалюты. Особенности правового регулирования и проблемы обеспечения информационной безопасности
13	Значение и правовое обеспечение государственной тайны. Рассматриваемые вопросы: - Подходы к опрепделению понятия «государственная тайна».

№ п/п	Тематика практических занятий/краткое содержание
	- Перечень сведений, составляющих государственную тайну. - Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей. Порядок установления степеней секретности. Распоряжение сведениями, составляющими государственную тайну. - Правовые механизмы допуска и доступа к сведениям, составляющим государственную тайну. - Система защиты государственной тайны. - Контроль и надзор за обеспечением защиты государственной тайны. Особенности правовой защиты сведений, составляющих государственную тайну.
14	Понятие и значение безопасности критической информационной инфраструктуры Рассматриваемые вопросы: - Правовые основы безопасности критической информационной инфраструктуры. - Значение федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ
15	Значение информационной безопасности на транспорте. Рассматриваемые вопросы: - Правовые основы безопасности критической информационной инфраструктуры. - Значение информационной безопасности на транспорте.
16	Значение международной информационной безопасности. Международный опыт борьбы с преступлениями в сфере компьютерной информации. Рассматриваемые вопросы: - Основы государственной политики РФ в области международной информационной безопасности. -Международный опыт борьбы с преступлениями в сфере компьютерной информации - Опыт борьбы с преступлениями в сфере компьютеной информации в зарубежных странах
17	Информационные правонарушения и преступления в информационной сфере Рассматриваемые вопросы: - Понятие и характеристика информационного правонарушения - Гражданско-правовая ответственность за информационные правонарушения.
18	Информационные правонарушения и преступления в информационной сфере. Рассматри ваемые вопросы: - Административные правонарушения в области связи и информации - Административно-правовая ответственность за информационные правонарушения.
19	Преступления в информационной сфере. Рассматри ваемые вопросы: - Уголовная ответственность за преступления в информационной сфере. Ответственность за преступления в сфере компьютерной информации. - Криминалистическая характеристика преступлений в сфере компьютерной информации.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом, литературой, нормативными и правовыми актами
2	Подготовка к промежуточной аттестации.
3	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8.	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 04.04.2022). - Текст : электронный
2	Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496492 (дата обращения: 04.04.2022). - Текст : электронный
3	Бартош, А. А. Основы международной безопасности. Организации обеспечения международной безопасности : учебное пособие для вузов / А. А. Бартош. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 320 с. — (Высшее образование). — ISBN 978-5-534-11783-7.	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493387 (дата обращения: 04.04.2022). - Текст : электронный
4	Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4.	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495922 (дата обращения: 04.04.2022). - Текст : электронный
5	Жарова, А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. — Москва : Издательство Юрайт, 2022. — 301 с. — (Актуальные монографии). — ISBN 978-5-534-14919-7.	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496939 (дата обращения: 04.04.2022). - Текст : электронный

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

Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru);

Единая коллекция цифровых образовательных ресурсов

(http://window.edu.ru);

Электронно-библиотечная система Лань (https://lanbook.ru/);

Образовательная платформа Юрайт (https://urait.ru/library/vo).

Научно-техническая библиотека РУТ (МИИТ) (http://library.miit.ru).

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

Microsoft Office,
Интернет-браузер,
СПС «Консультант Плюс».

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

Учебные аудитории для проведения занятий лекционного типа, оснащённые наборами демонстрационного оборудования.

Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещение для самостоятельной работы, оснащённые компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации

9. Форма промежуточной аттестации:

Экзамен в 7 семестре.

10. Оценочные материалы.

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

Авторы:

заведующий кафедрой, доцент, д.н. кафедры «Правовое обеспечение государственного управления и экономики» Юридического института А.А. Чеботарева

Согласовано:

Заведующий кафедрой АПЭПИП А.А. Чеботарева

Председатель учебно-методической комиссии М.Ю. Филиппова