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)

Преступления в сфере высоких технологий

Направление подготовки: 40.03.01 Юриспруденция

Направленность (профиль): Уголовно-правовой

Форма обучения: Очная

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:

-освоение норм материального и процессуального права в целях решения задач профессиональной деятельности в сфере высоких технологий;

-овладение профессиональной юридической лексикой в целях единообразного и корректного использования устной и письменной речи при квалификации преступлений в сфере высоких технологий;

-формирование навыков по реализации мероприятий по получению юридически значимой информации, проверки, анализу, оценки и ее применения в целях предупреждения, пресечения и раскрытия преступлений и иных правонарушений в сфере высоких технологий, в том числе - на транспорте.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен участвовать в экспертной юридической деятельности в рамках поставленной задачи.

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

Знать:

-нормы материального и процессуального права при решении задач профессиональной деятельности;

-профессиональную юридическую лексику.

Уметь:

-логически верно, аргументированно и ясно строить устную и письменную речь с единообразным и корректным использованием профессиональной юридической лексики;

-реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее ;

-использовать юридически значимую информацию в целях предупреждения, пресечения и раскрытия преступлений и иных правонарушений, в том числе - на транспорте.

Владеть:

-навыками применения норм материального и процессуального права;

-навыками логически верно, аргументированно и ясно строить устную и письменную речь с единообразным и корректным использованием профессиональной юридической лексики;

-навыками реализовывать мероприятия по получению юридически значимой информации в целях предупреждения, пресечения и раскрытия преступлений и иных правонарушений, в том числе - на транспорте.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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 №8
Контактная работа при проведении учебных занятий (всего):	50	50
В том числе:		
Занятия лекционного типа	10	10
Занятия семинарского типа	40	40

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 58 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, нормативно-правовое регулирование в сфере высоких технологий и информационной безопасности. Рассматриваемые вопросы: общие понятия и дефиниции, используемые в сфере высоких технологий и информационной безопас-ности; -классификация видов информации; -свойства и методы фиксации информации; -нормативно-правовое регулирование сферы высоких технологий и информационной безопасности.
2	Классификация преступлений в сфере высоких технологий и информационной безопасности. Рассматриваемые вопросы: -виды преступлений в сфере компьютерной информации; -уголовно-правовая характеристика неправомерного доступа к компьютерной информации; -особенности квалификации неправомерного доступа к компьютерной информации.
3	Создание, использование и распространение вредоносных компьютерных программ. Рассматриваемые вопросы: -понятие и виды вредоносных компьютерных программ; -уголовно-правовая характеристика создания, использования и распространения вредоносных ком-пьютерных программ; -особенности квалификации создания, использования и распространения вредоносных компьютерных программ.
4	Хищения, совершаемые в сфере высоких технологий. Рассматриваемые вопросы: -уголовно-правовая характеристика и особенности квалификации кражи денежных средств с банков-ского счета; -уголовно-правовая характеристика и особенности квалификации мошенничества с использованием электронных средств платежа; -уголовно-правовая характеристика и особенности квалификации мошенничества в сфере компью-терной информации.
5	Высокие технологии и информационные технологии в расследовании уголовных дел. Рассматриваемые вопросы: -компьютерная информация в доказывании по уголовным делам; -специфика производства следственных действий, направленных на изъятие электронных носителей информации и копирование компьютерной информации; -производство следственных действий, направленных на непосредственное получение компьютерной информации; -специфика доказывания при расследовании преступлений, совершаемых с использованием сети

№ п/п	Тематика лекционных занятий / краткое содержание
	Ин-тернет; -особенности назначения и производства судебной компьютерно-технической экспертизы.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Понятие, нормативно-правовое регулирование в сфере высоких технологий и информационной безопасности.Понятие, нормативно-правовое регулирование в сфере высоких технологий и информационной безопасности.Понятие, нормативно-правовое регулирование в сфере высоких технологий и информационной безопасности.Понятие, нормативно-правовое регулирование в сфере высоких технологий и информационной безопасности. Рассматриваемые вопросы: 1. Информация как объект правового регулирования. Структура информационной сферы и характери-стика ее элементов. Виды информации. 2. Правовые режимы конфиденциальной информации (персональные данные, служебная тайна, ком-мерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна). Юридическая ответственность за их нарушение. 3. Понятие и виды информационной безопасности. Информационная безопасность личности. Гаран-тии информационных прав граждан. Право на судебную защиту. 4. Информационная безопасность общества. Понятие информационной безопасности общества. Пра-вовое регулирование единого информационного пространства Российской Федерации. 5. Информационная безопасность государства. Понятие информационной безопасности государства. Обеспечение безопасности информационных и телекоммуникационных систем.
2	Понятие, нормативно-правовое регулирование в сфере высоких технологий и информационной безопасности. Рассматриваемые вопросы: 1. Международно-правовые основы криминализации преступлений в сфере высоких технологий и информационной безопасности. 2. Криминализация в уголовном законодательстве некоторых зарубежных стран преступлений в сфе-ре высоких технологий и информационной безопасности.
3	Классификация преступлений в сфере высоких технологий и информационной безопасности. Рассматриваемые вопросы: 1. Виды угроз информационной безопасности России: понятие и общая характеристика. 2. Общая характеристика и виды ответственности за правонарушения в информационной сфере. 3. Криминологическая характеристика преступности в области высоких технологий. 4. Криминалистическая характеристика компьютерных преступлений. 5. Международное сотрудничество в области борьбы с компьютерной преступностью.
4	Классификация преступлений в сфере высоких технологий и информационной безопасности. Рассматриваемые вопросы: 1. Многообразие способов совершения преступлений в сфере высоких технологий. 2. Классификация способов совершения компьютерных преступлений по законодательству России. 3. Сложность в квалификации деяний, совершенных в сфере высоких технологий.

№ п/п	Тематика практических занятий/краткое содержание
	4. Перечень смежных составов, предусматривающих неправомерное обращение с информацией по уголовному кодексу Российской Федерации.
5	Информационные отношения как объект уголовно-правовой охраны. Рассматриваемые вопросы: 1. Понятие родового объекта преступных посягательств в сфере высоких технологий; 2. Понятие предмета компьютерного преступления; 3. Понятие и виды преступлений в сфере высоких технологий.
6	Создание, использование и распространение вредоносных компьютерных программ. Рассматриваемые вопросы: 1. Понятие «вируса» и «вредоносной» компьютерной программы. 2. Понятие и способы распространения вредоносных компьютерных программ. 3. Понятие правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации и информационно-телекоммуникационных сетей. 4. Понятие правил эксплуатации и доступа к информационно-телекоммуникационным сетям.
7	Особенности квалификации преступлений в сфере высоких технологий и информационной безопасности. Рассматриваемые вопросы: 1.Особенности квалификации преступлений, предусмотренных ст. 272 УК РФ. 2.Особенности квалификации преступлений, предусмотренных ст. 272.1 УК РФ. 3.Особенности квалификации преступлений, предусмотренных ст. 273 УК РФ. 4.Особенности квалификации преступлений, предусмотренных ст. 274 УК РФ.
8	Уголовно-правовая характеристика преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки и передачи компьютерной информации и нарушения правил централизованного управления техническими средствами противодействия угрозам функционирования сети Интернет. Рассматриваемые вопросы: 1.Уголовно-правовая характеристика и особенности квалификации преступлений, связанных с нару-шением правил эксплуатации средств хранения, обработки и передачи компьютерной информации. 2.Уголовно-правовая характеристика неправомерного воздействия на критическую информационную инфраструктуры Российской Федерации. 3.Особенности квалификации преступлений, предусмотренных ст. 274.1 УК РФ. 4.Субъекты и объекты критической информационной инфраструктуры Российской Федерации. 5.Нарушение правил централизованного управления техническими средствами противодействия угрозам функционирования сети Интернет и сети связи общего пользования (ст. 274.2 УК РФ)
9	Посягательства на авторские и смежные права в компьютерных сетях. Рассматриваемые вопросы: 1. Уголовно-правовая характеристика посягательств на авторские и смежные права в компьютерных сетях. 2. Способы совершения посягательств на авторские и смежные права в компьютерных сетях. 3. Криминологическая характеристика посягательств на авторские и смежные права в компьютерных сетях. 4. Особенности расследования посягательств на авторские и смежные права в компьютерных сетях.
10	Хищения, совершаемые в сфере высоких технологий. Рассматриваемые вопросы: 1. Ообенности квалификации кражи денежных средств с банковского счета (п. «г» ч. 3 ст. 158 УК РФ). 2. Уоловно-правовая характеристика и особенности квалификации мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ).

№ п/п	Тематика практических занятий/краткое содержание
	3. Уголовно-правовая характеристика и особенности квалификации мошенничества в сфере компью-терной информации (ст. 159.6 УК РФ).
11	Преступления в сфере незаконного оборота наркотиков, совершаемые с использованием компьютерных технологий. Рассматриваемые вопросы: 1. Понятие незаконного сбыта наркотических средств и психотропных веществ посредством сети Ин-тернет или иных электронных сетей. 2. Уголовно-правовая характеристика незаконного оборота наркотических средств с использованием высоких технологий (ст. 228.1 УК РФ). 3. Особенности квалификации деяний, связанных с незаконным оборотом наркотических средств с использование высоких технологий. 4. Уголовно-правовая характеристика склонения к потреблению наркотических средств, психотроп-ных веществ или их аналогов с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет» ст. 230 УК РФ).
12	Преступления, совершаемые с использованием криптовалюты. Рассматриваемые вопросы: 1. Криптовалюта в системе платежных инструментов: понятие, место, особенности/ 2. Квалификация преступлений, совершаемых в отношении криптовалюты как предмета или объекта преступного посягательства. 3. Криптовалюта как средство совершения преступлений: вопросы уголовной ответственности. 4. Конфискация криптовалюты в рамках досудебного и судебного производства.
13	Преступления экстремистской направленности и террористического характера, совершаемые с использованием высоких технологий. Рассматриваемые вопросы: 1. Способы организации экстремистской и террористической деятельности с использованием высоких технологий. 2. Публичные призывы к осуществлению террористической деятельности, публичное оправдание тер-роризма или пропаганда терроризма (ст. 205.2 УК РФ). 3. Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207.1 УК РФ), заведомо ложной общественно значимой ин-формации, повлекшее тяжкие последствия (ст. 207.2 УК РФ). 4. Публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации (ст. 207.3 УК РФ). 5. Организация и финансирование деятельности экстремистской организации с использованием ин-формационных технологий (ст. 282.2, 282.3 УК РФ.).
14	Иные виды преступлений в сфере высоких технологий. Рассматриваемые вопросы: 1. Уголовно-правовая характеристика незаконной организации и проведения азартных игр с использованием информационно-телекоммуникационных сетей (ст. 171.2 УК РФ). 2. Уголовно-правовая характеристика преступлений против жизни и здоровья, совершаемых с использованием высоких технологий (ст.110, 110.1, 110.2 УК РФ и иные). 3. Уголовно-правовая характеристика возбуждения ненависти либо вражды, а равно унижения челове-ческого достоинства с использованием информационно-телекоммуникационных сетей (ст. 282 УК РФ). 4. Уголовно-правовая характеристика преступлений против половой свободы и половой неприкосно-венности, совершаемых с использованием информационно-телекоммуникационных сетей (ст. 133, 135, 242 УК РФ и иные).
15	Незаконный оборот специальных средств, предназначаемых для получения и модификации информации. Рассматриваемые вопросы:

№ п/п	Тематика практических занятий/краткое содержание
	1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. 2. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. 3. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем.
16	Высокие технологии и информационные технологии в расследовании уголовных дел. Рассматриваемые вопросы: 1. Особенности использования компьютерной информации в доказывании по уголовным делам. 2. Специфика производства следственных действий, направленных на изъятие электронных носителей информации и копирование компьютерной информации. 3. Производство следственных действий, направленных на непосредственное получение компьютер-ной информации. 4. Специфика доказывания при расследовании преступлений, совершаемых с использованием сети Интернет. 5. Особенности назначения и производства судебной компьютерно-технической экспертизы.
17	Криминалистическая деятельность по раскрытию и расследованию преступле-ний в сфере высоких технологий. Рассматриваемые вопросы: 1.Правовые, методические и организационные проблемы раскрытия. расследования и профилактики; 2. Вопросы использования специальных познаний.
18	Следовая картина информационных преступлений как отражение способа их совершения. Рассматриваемые вопросы: 1. Цифровые носители информации как место нахождения компьютерной информации. 2. Следы криминальной деятельности в преступлениях в сфере высоких технологий.
19	Методика расследования преступлений в сфере высоких технологий. Рассматриваемые вопросы: 1. Криминалистическая характеристика преступлений в сфере высоких технологий. 2. Типовые ситуации первоначального этапа расследования. 3. Специфика обращения с цифровыми носителями компьютерной информации. 4. Тактические особенности отдельных следственных действий.
20	Типология личности компьютерного преступника. Рассматриваемые вопросы: 1.Особенности субъектов компьютерных преступлений. 2. Классификация субъектов компьютерных преступлений. 3. Личностный аспект субъекта компьютерного преступления. Основные характеристики.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом, литературой, нормативными и правовыми актами.
2	Самостоятельное изучение тем дисциплины (модуля).
3	Подготовка к практическим занятиям.
4	Подготовка к промежуточной аттестации.

5	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Корабельников, С.М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С.М. Корабельников. — Москва: Изда-тельство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0.	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543351(дата об-ращения 28.04.2025) — Текст: электрон-ный
2	Криминология : учебник для вузов / под общей редакцией О.С. Капинус. — 2-е изд., перераб. и доп. — Москва : Изда-тельство Юрайт, 2025. — 1132 с. — (Высшее образование). — ISBN 978-5-534-09795-5.	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/565567 (дата обращения 28.04.2025) — Текст: элек-тронный
3	Преступления в сфере высоких техноло-гий и информационной безопасности : учебное пособие / В.Ф. Васюков, А.Г. Волеводз, М.М. Долгиева, В.Н. Чаплы-гина; под науч. ред. А.Г. Волеводза. — Москва: Прометей, 2023. — 1086 с. — SBN 978-5-00172-447-6.	Образовательная платформа Знаниум [сайт]. — URL: https://znanium.ru/catalog/product/2124867 (дата обращения 28.04.2025) — Текст: электронный
4	Преступления в сфере высоких техноло-гий и информационной безопасности : учебное пособие / В.Ф. Васюков, А.Г. Волеводз, М.М. Долгиева, В.Н. Чаплы-гина; под науч. ред. А.Г. Волеводза. — Москва: Прометей, 2023. — 1086 с. — SBN 978-5-00172-447-6.	Образовательная платформа Знаниум [сайт]. — URL: https://znanium.ru/catalog/product/2124867 (дата обращения 28.04.2025) — Текст: электронный

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

Официальный интернет-портал правовой информации – www.pravo.gov.ru

Государственная автоматизированная система Российской Федерации «Правосудие» интернет-портал – https://sudrf.ru/

Российское агентство правовой и судебной информации – https://rapsinews.ru/

Конституционный Суд Российской Федерации – https://ksrf.ru/ru/Pages/default.aspx

Образовательная платформа Юрайт - https://urait.ru

СПС «Консультант Плюс» - https://www.consultant.ru/

Верховный Суд Российской Федерации –https://vsrf.ru/

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

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 Windows;

Microsoft Office;

Интернет-браузер,

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Webinar.ru, Среда электронного обучения Русский Moodle, электронная почта и т.п.

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

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

Помещение для самостоятельной работы, оснащённое компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

9. Форма промежуточной аттестации:

Экзамен в 8 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, доцент, к.н. кафедры «Уголовное право, уголовный процесс и правоохранительная деятельность» Юридического института Е.А. Царева

Согласовано:

и.о. заведующего кафедрой УПиПД А.М. Репьева

Председатель учебно-методической комиссии Е.Н. Рудакова