

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 магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Правовые основы обеспечения информационной безопасности

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

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: 4196
Подписал: заведующий кафедрой Желенков Борис
Владимирович
Дата: 19.10.2022

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» является формирование компетенций по основным разделам теоретических и практических основ применения законодательных актов РФ при разработке и эксплуатации систем обеспечения информационной безопасности на транспорте.

Основными задачами дисциплины являются:

- Ознакомление с законодательными актами и нормативно-правовым обеспечением информационной безопасности на транспорте;
- Изучение особенностей практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности на транспорте.
- Изучение технических и организационных методов практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности на транспорте.
- Изучение методов построения систем обеспечения информационной безопасности с учетом законодательных актов и нормативно-правового обеспечения.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность

- Анализ требований нормативно-правовых актов к разработке и эксплуатации политик и систем информационной безопасности;
- Анализ технических и организационных методов практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности на транспорте;
- Анализ действующих систем обеспечения информационной безопасности и опыта их эксплуатации.

Проектная деятельность

- Проектирование политик информационной безопасности предприятия с учетом требований российского законодательства и ведомственных нормативно-правовых актов, а также документов для их реализации;
- Разработка и оформление документов, регламентирующих деятельность служб обеспечения информационной безопасности предприятия;
- Контроль соответствия действующих систем информационной безопасности и документации, регламентирующей их эксплуатацию,

российскому законодательству.

Организационно-управленческая деятельность

- Разработка организационных методов реализации политики безопасности предприятия при проектировании системы информационной безопасности;

- Организация и управление коллективной разработкой системы обеспечения информационной безопасности предприятия с учетом современных средств и технологий в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

ПК-6 - Способность организовать работу по созданию, модернизации и сертификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.

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

Знать:

- основные законодательные акты и нормативно-правовое обеспечение информационной безопасности на транспорте;

- средства и технологии обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России .

Уметь:

- разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

- организовать работу по созданию, модернизации и сертификации систем, средств и технологий обеспечения информационной безопасности.

Владеть:

- навыками разработки и оформления документов, регламентирующих

деятельность служб обеспечения информационной безопасности предприятия;
-навыками проектирования политик информационной безопасности предприятия с учетом требований российского законодательства и ведомственных нормативно-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	Сем. №4
Контактная работа при проведении учебных занятий (всего):	24	24
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	8	8

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 120 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	<p>1 Информационная безопасность: сущность и содержание Рассматриваемые вопросы: -Информация как один из наиболее важных ресурсов современности. --Информационная безопасность в системе национальной безопасности. -Понятие информационной безопасности как состояния защищенности жизненно важных интересов личности, общества и государства в информационной сфере. -Разграничение понятий «информационная безопасность», «компьютерная безопасность» и «защита информации». -Правовой, организационный и программно-технический уровни обеспечения информационной безопасности. -Проблемы разработки и внедрения методов и средств обеспечения информационной безопасности в государственных организациях и коммерческих предприятиях России.</p> <p>2 Государственная политика в сфере обеспечения информационной безопасности Рассматриваемые вопросы: -Понятие государственной политики в информационной сфере. -Основные положения государственной политики в сфере информационной безопасности. -Обеспечение равенства участников процесса информационного взаимодействия. -Совершенствование нормативно-правовой базы регулирования информационных отношений. -Контроль за соблюдением и исполнением законодательства в информационной сфере. -Развитие современных информационных и телекоммуникационных технологий как одна из приоритетных задач государственной политики в сфере информационной безопасности. -Государственная политика в сфере обеспечения информационной безопасности на транспорте. -Национальная Программа "Цифровая экономика Российской Федерации". -Национальные проекты в сфере цифровизации.</p> <p>3 Основные задачи обеспечения информационной безопасности Рассматриваемые вопросы: -Обеспечение информационной безопасности как комплексная задача. -Создание системы органов, ответственных за информационную безопасность. -Разработка теоретико-методологической основы обеспечения безопасности информации. -Создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения информационной безопасности. -Организация подготовки специалистов по защите информации. -Решение проблемы управления защитой информации и ее автоматизация. -Общие задачи обеспечения информационной безопасности. -Режим государственной, коммерческой, личной (семейной) тайны. -Частные задачи обеспечения информационной безопасности. -Обеспечение безопасности функционирования информационных систем. -Разработка стратегии обеспечения информационной безопасности России. -Обоснование государственной политики в условиях глобализации информационных процессов, формирования геоинформационных сетей. -Разработка научно-практических основ формирования и проведения государственной политики в области обеспечения информационной безопасности. -Обоснование приоритетов национальной безопасности, соответствующих долговременным интересам общественного развития. -Реализация национальных проектов в сфере цифровизации в проекте Минтранса «Цифровой транспорт и логистика».</p>

№ п/п	Тематика лекционных занятий / краткое содержание
4	<p>Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности. Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> • Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» • Федеральный закон № 152-ФЗ «О персональных данных». • Доктрина информационной безопасности Российской Федерации • Федеральный закон N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". • Федеральный закон Российской Федерации N 98-ФЗ "О коммерческой тайне" <p>-Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.</p> <p>-Обладатель информации, его права и обязанности.</p> <p>-Конфиденциальность персональных данных.</p> <p>- Согласие субъекта персональных данных на обработку его персональных данных.</p> <p>-Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных.</p> <p>-Угрозы информационной безопасности РФ.</p> <p>-Угрозы информационному обеспечению государственной политики РФ.</p> <p>-Угрозы развитию отечественной индустрии информации.</p> <p>-Угрозы безопасности информационных и телекоммуникационных средств и систем.</p> <p>- Принципы Государственная политика обеспечения информационной безопасности.</p> <p>-Принципы обеспечения безопасности критической информационной инфраструктуры.</p> <p>- Полномочия Президента РФ и органов государственной власти РФ в области обеспечения безопасности критической информационной инфраструктуры.</p> <p>- Категорирование объектов критической информационной инфраструктуры.</p> <p>-Система безопасности значимого объекта критической информационной инфраструктуры.</p> <p>5</p> <p>Основные задачи обеспечения информационной безопасности. Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Организационно-технические, экономические и правовые методы. -Этапы обеспечения ИБ на предприятии. -Создание режима охраны информации; разработка правил взаимоотношений между сотрудниками; регламентация работы с документами; правила использования технических средств в рамках существующего правового поля РФ; аналитическая работа по оценке угроз информационной безопасности. -Обязанности руководства организации по обеспечению ИБ (ISO 27001) -Создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения информационной безопасности. -Организация подготовки специалистов по защите информации. -Решение проблемы управления защитой информации и ее автоматизации. <p>6 Угрозы информационной безопасности</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> -Понятие угрозы информационной безопасности. -Виды угроз информационной безопасности. -Информационное оружие и направления его применения. -Информационные войны. -Внешние и внутренние угрозы информационной безопасности.

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>-Компьютерные сети и информационная безопасность.</p> <p>- Понятие и виды атак на компьютерную систему.</p> <p>-Классификация атак на компьютерную систему.</p> <p>-Вредоносные программы, их виды и направления применения</p> <p>-Понятие и виды антивирусного программного обеспечения.</p> <p>-Правовой, организационный и программно-технический способы нейтрализации угроз информационной безопасности.</p> <p>-Программно-Технические средства защиты информации</p> <p>-Аутентификация и идентификация.</p> <p>-Организационные средства защиты информации.</p> <p>-Электронная подпись.</p> <p>-Простая, усиленная неквалифицированная, усиленная квалифицированная электронные подписи.</p> <p>7 Формирование нормативно-правовой базы обеспечения информационной безопасности.</p> <p>Рассматриваемые вопросы:</p> <p>-Разработка нормативно-правовых и организационно-методических документов, регламентирующих деятельность органов государственной власти в области информационной безопасности; взаимоотношения субъектов информационной деятельности в части обеспечения информационной безопасности.</p> <p>-Государственная регламентация процессов функционирования и развития рынка средств информации, информационных продуктов и услуг.</p> <p>-Разработка концепции информационной безопасности.</p> <p>-Регулирование правового статуса субъектов системы информационной безопасности, пользователей информационных и телекоммуникационных систем.</p> <p>-Силы обеспечения информационной безопасности</p> <p>8</p> <p>Развитие современных методов обеспечения информационной безопасности</p> <p>Рассматриваемые вопросы:</p> <p>-Разработка методов комплексного исследования деятельности персонала информационных систем.</p> <p>-Разработка практических рекомендаций по сохранению и укреплению политической стабильности в обществе; обеспечению прав и свобод граждан; укреплению законности и правопорядка методами информационной безопасности.</p> <p>-Формирование подходов и способов обеспечения органов государственной власти и управления, граждан и их объединений достоверной, полной и своевременной информацией.</p> <p>-Выработка основных направлений деятельности по предотвращению негативных информационных воздействий на индивидуальное, групповое и общественное сознание.</p> <p>9 ГОСТы РФ в области информационной безопасности.</p> <p>Рассматриваемые вопросы:</p> <p>-ГОСТ Р 50922, ГОСТ Р 51275, ГОСТ Р ИСО/МЭК 15408, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 13335, ГОСТ Р ИСО/ТО 13569, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 18044, ГОСТ Р ИСО/МЭК 18045, ГОСТ Р ИСО/МЭК 19794, ГОСТ Р 50739, ГОСТ Р 51188, ГОСТ Р 51725.6, ГОСТ Р 51898, ГОСТ Р 52069, ГОСТ Р 52447, ГОСТ 28147, ГОСТ Р 34.10, ГОСТ Р 34.11</p> <p>-Стандарты в области ИБ организаций банковской системы РФ: СТО БР ИББС-1.0/1.1, РС БР ИББС-2.0/2.1/2.2</p> <p>-ГОСТы серии ГОСТ Р ИСО/МЭК 2700 «Информационные технологии.</p> <p>-Методы обеспечения безопасности.</p> <p>-Менеджмент информационной безопасности».</p> <p>10 Проблемы повышения эффективности обеспечения информационной безопасности на современном этапе</p> <p>Рассматриваемые вопросы:</p>

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>-Обеспечение согласованности решений органов, ответственных за реализацию государственной политики в сфере обеспечения информационной безопасности в рамках единого информационного пространства.</p> <p>-Политика протекционизма, направленная на поддержку деятельности отечественных производителей средств информатизации и защиты информации.</p> <p>-Защита внутреннего рынка от проникновения некачественных средств информатизации и информационных продуктов.</p> <p>-Необходимость формирования программы информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности.</p>

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	<p>1. Защита персональных данных. ФЗ №152 и ГОСТы РФ. В результате выполнения практического задания студент получает навыки в практическом применении законодательных норм для защиты персональных данных (ФЗ №152, Приказ ФСБ от 10.07.2014 № 378, Приказ ФСТЭК от 11.02.2013 №17, Приказ ФСТЭК от 18.02.2013 №21 и пр.)</p> <p>2. Способы защиты коммерческой тайны. ФЗ №98 и ГОСТы РФ. В результате выполнения практического задания студент получает навыки в практическом применении законодательных норм для защиты коммерческой тайны (ФЗ №98, Указ Президента РФ № 188 и пр.)</p> <p>3. Методы и средства защиты информации. Российские и международные стандарты. В результате выполнения практического задания студент получает навыки в практическом применении российских и международных стандартов в области методов и средств защиты информации (ISO/IEC 27000, ГОСТ ИСО/МЭК 15408 и пр.)</p> <p>4. Организация службы информационной безопасности на предприятии. В результате выполнения практического задания студент получает навыки в практической организации работы службы ИБ (разграничение обязанностей, подготовка инструкций, взаимодействие служб и их функционал и пр.)</p>

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	<p>1 Работа с лекционным материалом</p> <p>2 Подготовка к практическим занятиям</p> <p>3 Изучение вопросов для самостоятельной дополнительной проработки</p>
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	Леонтьев. Защита информации: учебное пособие. МИРЭА - Российский технологический университет, 2021.-79с	https://e.lanbook.com/book/182491 (дата обращения: 04.10.2022)
2	Лагоша О. Н. Сертификация информационных систем. М.: Издательство "Лань", 2021.-112с	https://e.lanbook.com/book/156616 (дата обращения: 04.10.2022)
3	Прохорова О. В. Информационная безопасность и защита информации: учебник для СПО. М.: Издательство "Лань", 2021.-124с	https://e.lanbook.com/book/158939 (дата обращения: 04.10.2022)
4	Груздева Л. М. Российский университет транспорта, 2019.-144с	https://e.lanbook.com/book/188703 (дата обращения: 04.10.2022)
5	Титова Л. Н. Информационная безопасность и защита информации: учебно-методическое пособие. Башкирский государственный педагогический университет им. М. Акмуллы, 2013.-108с	https://e.lanbook.com/book/56704 (дата обращения: 04.10.2022)
6	Моргунов А.В. Информационная безопасность: учебно-методическое пособие. Новосибирский государственный технический университет, 2019-83с	https://e.lanbook.com/book/152227 (дата обращения: 04.10.2022)

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

- Форум специалистов по информационным технологиям
<http://citforum.ru/>
- Интернет-университет информационных технологий
<http://www.intuit.ru/>
- Тематический форум по информационным технологиям
<http://habrahabr.ru/>
- ЭБС "Лань" <https://e.lanbook.com/book/>

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

- Microsoft Windows
- Microsoft Office

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий может потребоваться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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

-Учебная аудитория для проведения занятия лекционного типа, групповых и индивидуальных консультации. Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером. Аудитория подключена к интернету МИИТ.

-Учебная аудитория для проведения лабораторных работ. Персональные компьютеры.

- В случае проведения занятия с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Экзамен в 4 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
«Вычислительные системы, сети и
информационная безопасность»

Малинский
Станислав
Вальтерович

Лист согласования

Заведующий кафедрой ВССиИБ
Председатель учебно-методической
комиссии

Б.В. Желенков

Н.А. Клычева