**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
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## Организационное и правовое обеспечение информационной безопасности

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность 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: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 26.10.2022

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Организационное и правовое обеспечение информационной безопасности» является формирование компетенций по основным разделам теоретических и практических основ применения законодательных актов РФ при разработке и эксплуатации систем обеспечения информационной безопасности.

Основными задачами дисциплины являются:

• Ознакомление с законодательными актами и нормативно-правовым обеспечением информационной безопасности;

• Изучение особенностей практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности.

• Изучение технических и организационных методов практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности.

• 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):

Эксплуатационная деятельность

• Сбор и анализ данных для проектирования и совершенствования систем информационной безопасности предприятий;

• Сбор и анализ данных для аудита и оценки эффективности работы служб информационной безопасности;

• Разработка и оформление документации, регламентирующей деятельность служб информационной безопасности;

• Контроль соответствия разрабатываемой документации стандартам, техническим условиям и другим нормативным документам.

Проектно-технологическая деятельность

• Проектирование политик информационной безопасности предприятия с учетом требований российского законодательства и ведомственных нормативно-правовых актов, а также документов для их реализации;

• Проектирование систем информационной безопасности в соответствии с законодательными и нормативными документами.

Экспериментально-исследовательская деятельность

• Анализ требований к разрабатываемому обеспечению информационной безопасности предприятий;

• Исследование функциональных требований к разрабатываемым системам информационной безопасности;

• Исследование эффективности действующих систем информационной безопасности.

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-5** - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности ;

**ОПК-6** - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ;

**ПК-14** - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

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 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 | Сем. №7 |
| Контактная работа при проведении учебных занятий (всего): | 48 | 48 |
| В том числе: | | |
| Занятия лекционного типа | 32 | 32 |
| Занятия семинарского типа | 16 | 16 |

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 60 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 | 1. Информационная безопасность: сущность и содержание<br>Рассматриваемые вопросы:<br>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.<br>Проблемы разработки и внедрения методов и средств обеспечения информационной безопасности в государственных организациях и коммерческих предприятиях России.<br><br>2. Государственная политика в сфере обеспечения информационной безопасности<br>Рассматриваемые вопросы:<br>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 законодательства в информационной сфере. Национальная Программа "Цифровая экономика Российской Федерации". Национальные проекты в сфере цифровизации.<br><br>3. Основные задачи обеспечения информационной безопасности<br>Рассматриваемые вопросы:<br>Обеспечение информационной безопасности как комплексная задача.<br>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.<br>Организация подготовки специалистов по защите информации. Решение проблемы управления защитой информации и ее автоматизация.<br>Общие задачи обеспечения информационной безопасности. Режим государственной, коммерческой, личной (семейной) тайны. Разработка стратегии обеспечения информационной безопасности России.<br><br>4. Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности<br>Рассматриваемые вопросы:<br>• Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | информации»<br>• Федеральный закон № 152-ФЗ «О персональных данных».<br>• Доктрина информационной безопасности Российской Федерации<br>• Федеральный закон N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".<br>• Федеральный закон Российской Федерации N 98-ФЗ "О коммерческой тайне"<br>Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. Обладатель информации, его права и обязанности.<br>Конфиденциальность персональных данных. Согласие субъекта персональных данных на обработку его персональных данных.<br>Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных.<br>Угрозы развитию отечественной индустрии информации. Принципы обеспечения безопасности критической информационной инфраструктуры. Категорирование объектов критической информационной инфраструктуры. Система безопасности значимого объекта критической информационной инфраструктуры<br><br>5. Основные задачи обеспечения информационной безопасности. Организационно-технические, экономические и правовые методы<br>Рассматриваемые вопросы:<br>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.<br>Обязанности руководства организации по обеспечению ИБ (ISO 27001)<br>Создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения информационной безопасности.<br><br>6. Угрозы информационной безопасности<br>Рассматриваемые вопросы:<br>Понятие угрозы информационной безопасности. Виды угроз информационной безопасности. Внешние и внутренние угрозы информационной безопасности. Компьютерные сети и информационная безопасность. Понятие и виды атак на компьютерную систему. Классификация атак на компьютерную систему.<br>Вредоносные программы, их виды и направления применения.<br>Понятие и виды антивирусного программного обеспечения.<br>Правовой, организационный и программно-технический способы нейтрализации угроз информационной безопасности.<br>Аутентификация и идентификация. Организационные средства защиты информации. Электронная подпись. Простая, усиленная неквалифицированная, усиленная квалифицированная электронные подписи.<br><br>7. Формирование нормативно-правовой базы обеспечения информационной безопасности<br>Рассматриваемые вопросы:<br>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.<br>Государственная регламентация процессов функционирования и развития рынка средств информации, информационных продуктов и услуг. Разработка концепции информационной безопасности. |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | 8. Развитие современных методов обеспечения информационной безопасности<br>Рассматриваемые вопросы:<br>Разработка методов комплексного исследования деятельности персонала информационных систем.<br>Разработка практических рекомендаций по сохранению и укреплению политической стабильности в обществе; обеспечению прав и свобод граждан; укреплению законности и правопорядка методами информационной безопасности.<br>Формирование подходов и способов обеспечения органов государственной власти и управления, граждан и их объединений достоверной, полной и своевременной информацией.<br><br>9. ГОСТы РФ в области информационной безопасности.<br>Рассматриваемые вопросы:<br>Стандарты в области ИБ организаций банковской системы РФ: СТО БР ИББС-1.0/1.1, РС БР ИББС-2.0/2.1/2.2.<br>ГОСТы серии ГОСТ Р ИСО/МЭК 2700 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности».<br><br>10. Проблемы повышения эффективности обеспечения информационной безопасности на современном этапе<br>Рассматриваемые вопросы:<br>Обеспечение согласованности решений органов, ответственных за реализацию государственной политики в сфере обеспечения информационной безопасности в рамках единого информационного пространства.<br>Политика протекционизма, направленная на поддержку деятельности отечественных производителей средств информатизации и защиты информации. Защита внутреннего рынка от проникновения некачественных средств информатизации и информационных продуктов. |

## 4.2. Занятия семинарского типа.

## Практические занятия

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 1 | 1 Защита персональных данных. ФЗ №152 и ГОСТы РФ.<br>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.)<br><br>2 Способы защиты коммерческой тайны. ФЗ №98 и ГОСТы РФ.<br>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.)<br><br>3 Методы и средства защиты информации. Российские и международные стандарты.<br>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.)<br><br>4 Организация службы информационной безопасности на предприятии.<br>В результате выполнения практического задания студент получает навыки в практической организации работы службы ИБ (разграничение обязанностей, подготовка инструкций, |

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| | взаимодействие служб и их функционал и пр.) |

4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|---|---|
| 1 | Работа с лекционным материалом |
| 2 | Подготовка к практическим занятиям |
| 3 | Подготовка к промежуточной аттестации. |
| 4 | 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: 02.10.2022).-Текст электронный |
| 2 | Груздева Л. М. Российский университет транспорта, 2019.-144с | https://e.lanbook.com/book/188703(дата обращения: 02.10.2022).-Текст электронный |
| 3 | 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: 02.10.2022).-Текст электронный |
| 4 | Моргунов А.В. Информационная безопасность: учебно-методическое пособие. Новосибирский государственный технический университет, 2019- 83с | https://e.lanbook.com/book/152227(дата обращения: 02.10.2022).-Текст электронный |

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 проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться 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 занятий лекционного типа, групповых и индивидуальных консультаций.

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером (CP UCorei3, 8GBRAM, 1Tb HDD, GeForce GTSeries). Аудитория подключена к интернету МИИТ.

- Учебная аудитория для проведения практических работ.

персональные компьютеры (процессор intelPentium 2.3 Ghz, 1 Гб оперативной памяти)

В случае проведении занятий 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:

Зачет в 7 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» С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической комиссии Н.А.Клычева