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
09.03.02 Информационные системы и технологии,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности

Направление подготовки: 09.03.02 Информационные системы и технологии

Направленность (профиль): Информационные системы и технологии на транспорте

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью дисциплины «Основы информационной безопасности» является формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты. Приобретенные знания позволят студентам правильно ориентироваться в категориях защищаемых информационных ценностей и приобрести минимально необходимый кругозор в проблемах информационной безопасности. На основе данной дисциплины предполагается более подробно изучать различные направления защиты компьютерной безопасности.

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

Производственно-технологическая деятельность

- Разработка методов и средств технической защиты информации;
- Разработка технологических решений для обеспечения информационной безопасности в различных сферах.

Организационно-управленческая деятельность

- Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;
- Разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;
- Организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач.

Проектная деятельность

- Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации;
- Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации;
- Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации.

- Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации;

- Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации;

- Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;.

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

Знать:

-сущность и понятие информационной безопасности, характеристику ее составляющих;

-место информационной безопасности в системе национальной безопасности страны;

- виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению;

-факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

- современные средства и способы обеспечения информационной безопасности;

-основные методики анализа угроз и рисков информационной безопасности.

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;

-классифицировать основные угрозы безопасности информации.

Владеть:

-профессиональной терминологией;

- навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и объектов информатизации;

- методами защиты информации.

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):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

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 80 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	Основные понятия и задачи информационной безопасности. Рассматриваемые вопросы: - понятие информации и информационной безопасности; - информация, сообщения, информационные процессы как объекты информационной безопасности, обзор защищаемых объектов и систем; -понятие «угроза информации», понятие «риска информационной безопасности»; - сущность функционирования системы защиты информации; защита человека от опасной информации и от не информированности в области информационной безопасности.
2	Основы защиты информации Рассматриваемые вопросы: - целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности; - понятия государственной тайны и конфиденциальной информации, жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации; - основные понятия в области защиты информации, элементы процесса менеджмента ИБ; - модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.
3	Угрозы безопасности защищаемой информации Рассматриваемые вопросы: - понятие угрозы безопасности информации, каналы и методы несанкционированного доступа к информации; - уязвимости, методы оценки уязвимости информации.
4	Методологические подходы к защите информации Рассматриваемые вопросы: - анализ существующих методик определения требований к защите информации; - параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации; - виды мер и основные принципы защиты информации.
5	Нормативно правовое регулирование защиты информации Рассматриваемые вопросы: -организационная структура системы защиты информации, законодательные акты в области защиты информации; - российские и международные стандарты, определяющие требования к защите информации; - система сертификации РФ в области защиты информации, основные правила и документы системы сертификации РФ в области защиты информации.
6	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации. Рассматриваемые вопросы: -основные механизмы защиты информации, система защиты информации, меры защиты информации, реализуемые в автоматизированных (информационных) системах; - программные и программно-аппаратные средства защиты информации, инженерная защита и техническая охрана объектов информатизации; - организационно-распорядительная защита информации, работа с кадрами и внутри объектовый режим, принципы построения организационно-распорядительной системы.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Основы защиты информации. В результате выполнения лабораторной работы студент получает: - определение объектов защиты на типовом объекте информатизации; -классификация защищаемой информации по видам тайны и степеням конфиденциальности; -основные признаки присутствия на компьютере вредоносных программ.
2	Угрозы безопасности защищаемой информации В результате выполнения лабораторной работы студент получает: -классификация защищаемой информации по видам тайны и степеням конфиденциальности; - сетевая активность.
3	Нормативно правовое регулирование защиты информации В результате выполнения лабораторной работы студент получает: -работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности; -защита от несанкционированных хакерских атак.
4	Система сертификации РФ в области защиты информации В результате выполнения лабораторной работы студент получает: -выбор мер защиты информации для автоматизированных рабочих мест; -управление правами пользователей в Windows.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Выполнение индивидуального задания по теме: «Примеры преступлений в сфере информации и информационных технологий»
3	Выполнение индивидуального задания по теме: «Информационные технологии и защиты информации»
4	Выполнение курсовой работы.
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Формы психологической защиты человека от информационной перегрузки.

2. Социально вредная информация в СМИ.

3. Вредная и опасная информация в Интернет

4. Формы обмана и мошенничества в Интернет.

5. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.

6. Модель информационной защиты каналов связи.

7. Стратегия обмана и ее использование в сфере информационной защиты.

8. Вопросы информационной безопасности в политике и дипломатии.

9. Организационно-распорядительные меры информационной защиты.

10. Традиционные направления информационной защиты и пути их интеграции.

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

№ п/п	Библиографическое описание	Место доступа
1	Основы информационной безопасности : курс лекций / В.А. Галатенко; Ред. В.Б. Бетелин. - М. : Интернет-Университет Информационных Технологий, 2003. - 280 с. - (Основы информационных технологий). - ISBN 5-9556-0003-5 :	НТБ РУТ (МИИТ)
2	Конституция РФ от 12.12.93 (с изм. и доп. от 10.02.1996).	НТБ РУТ (МИИТ)
3	ФЗ «Об информации, информационных технологиях и защите информации», № 149-ФЗ от 27.07.2006.	НТБ РУТ (МИИТ)
4	ФЗ «О персональных данных», № 152-ФЗ от 27.07.2006	НТБ РУТ (МИИТ)

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

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

Официальный сайт по поддержке решений Cisco https://www.cisco.com/

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Тематический форум по информационным технологиям http://habrahabr.ru/.

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

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

Для проведения лабораторных работ необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными 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).

Для проведения аудиторных занятий и самостоятельной работы требуются:

- Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET

- Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

- Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения практических занятий:

- компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

- 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 3 семестре.

Курсовая работа в 3 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
«Вычислительные системы, сети и
информационная безопасность» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ЦТУТП В.Е. Нутович

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова