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
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Технологии разработки программного обеспечения

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Дисциплина посвящена изучению основ информационной безопасности. В дисциплине предусмотрено изучение пяти учебных тем, объединенных единым замыслом. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. На основе единого подхода рассматриваются девять исторически сложившихся направлений информационной защиты. Излагаются разработанные или модифицированные автором качественные модели информационной защиты. Завершается изучение дисциплины двумя темами, посвященными двум наиболее существенным угрозам информационной безопасности – информационным преступлениям и информационным войнам. В рамках, указанных тем приводится классификация информационных и компьютерных преступлений, объясняются их причины, дается уголовно-правовая характеристика некоторых преступных деяний, рассматриваются основные стратегии информационных войн и виды информационного оружия.

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	Сем. №3
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 Содержание учебного материала: -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 Содержание учебного материала: -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

№ п/п	Тематика лекционных занятий / краткое содержание
	Содержание учебного материала: -Понятие угрозы безопасности информации. -Понятие угрозы безопасности информации. -Каналы и методы несанкционированного доступа к информации. -Уязвимости. -Методы оценки уязвимости информации.
4	Методологические подходы к защите информации Содержание учебного материала: -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 Содержание учебного материала: -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 Содержание учебного материала: - 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	Основные признаки присутствия на компьютере вредоносных программ. В результате выполнения лабораторной работы студент получит навыки классификации информационных активов по видам угроз и классам защищенности, а также навыки обнаружения вредоносного программного кода на персональном компьютере.
2	Обнаружение сетевой активности В результате выполнения лабораторной работы студент получит навыки обнаружения сетевой активности в защищаемой системе.
3	Защита от несанкционированного доступа и сетевых хакерских атак В результате выполнения лабораторной работы студент получит навыки работы встроенным брандмауэром Microsoft Windows.
4	Защита информации для автоматизированных рабочих мест. Управление правами

№ п/п	Наименование лабораторных работ / краткое содержание
	пользователей в Windows В результате выполнения лабораторной работы студент получает навыки базовой настройки компонентов АРМ для обеспечения ИБ.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
3	Подготовка индивидуального задания
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	Яковлев, Валентин Васильевич. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта : учебник для студ. вузов ж.-д. трансп. / В.В. Яковлев, А.А.Корниенко. - М. : УМК МПС России, 2002. - 328 с. : ил. - ISBN 5-89035-059-5 : 64.55 р	научно-техническая библиотека МИИТ(дата обращения 12.03.2023)полочный шифр 656.2-Я47Текст : непосредственный.
2	Голдовский, Яков Михайлович. Структуры и организация данных : метод. указ. к практ. занятиям для спец. "Вычислит. машины, комплексы, системы и сети" ИУИТ / Я.М. Голдовский ; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2005. - 30 с. 24.53 р.	URL:http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/04-35329.pdf.Текст : непосредственный.Полочный шифр 004-Г60(дата обращения 12.03.2023)
3	Голдовский, Яков Михайлович. Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц.	URL:http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf.Полочный шифр 004-Г60. (дата обращения 12.03.2023) [Электронный ресурс]

	"Теоретические основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / Я. М. Голдовский, Б. В. Желенков, И. Е. Сафонова ; МИИТ. Каф. "Вычислительные системы и сети". - М. : МГУПС(МИИТ), 2013. - 36 с. : ил.. - Библиогр.: с. 46. - 100 экз. - (в пер.) : 39.78 р. - Текст : непосредственный.	

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
- 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. Клычева