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 специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины (модуля) «Основы информационной без-опасности» являются: – обучить студентов принципам обеспечения информационной безопасности, подходам к анализу информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем; – содействовать фундаментализации образования, формированию научного миро-воззрения и развитию системного мышления. Задачи изучения дисциплины: - изучение основных методов и принципов обеспечения конфиденциальности, це-лостности и доступности информации в компьютерных системах; - изучение типовых угроз безопасности информации при её обработке в компью-терных системах; - изучение основных принципов обеспечения информационной безопасности; - изучение основ построения модели угроз и политики безопасности; - изучение основных моделей управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

ПК-1 - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах.

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

Владеть:

Понимает значение информации и информационной безопасности в развитии современного общества, значимость своей будущей профессии.

Владеть:

Владеет методами и средствами моделирования политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации

Знать:

Знает типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации.

Уметь:

Умеет адаптировать типовые и строить оригинальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.

Уметь:

Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.

Знать:

Изучает и анализирует отечественный и зарубежный опыт по проблемам компьютерной безопасности.

Уметь:

Участвует в проведении экспериментально-исследовательских работ при сертификации средств 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. №4
Контактная работа при проведении учебных занятий (всего):	72	72
В том числе:		
Занятия лекционного типа	36	36
Занятия семинарского типа	36	36

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 72 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	Информационная безопасность в системе национальной безопасности Российской Федерации
2	Понятие национальной безопасности. Сущность и содержание национальной безопасности. Основные задачи в области обеспечения национальной безопасности. Объект и субъект безопасности. Виды безопасности. Виды защищаемой информации. Основные понятия и общеметодологические принципы информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства
3	Национальные интересы России в информационной сфере. Место и роль России в глобальном информационном пространстве. Национальные интересы России в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
4	Виды угроз информационной безопасности Российской Федерации. Проблемы обеспечения информационной безопасности. Угрозы конституционным правам и

№ п/п	Тематика лекционных занятий / краткое содержание
	свободам человека и гражданина. Угрозы информационному обеспечению государственной политики РФ. Угрозы развитию отечественной индустрии информации, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Классификация угроз безопасности информационных и телекоммуникационных средств и систем. Модель действий нарушителя.
5	Источники угроз информационной безопасности РФ. Внешние источники угроз. Внутренние источники угроз. Классификация источников угроз и уязвимостей информационной безопасности.
6	Информационная война, методы и средства её ведения
7	Информационная безопасность и информационное противоборство. Понятие информационной войны. Проблемы информационных войн. Субъекты информационного противоборства. Цель информационного противоборства. Составные части и методы информационного противоборства
8	Приемы информационного воздействия в информационной войне. Информационная война как целенаправленное информационное воздействие информационных систем. Способы перепрограммирования информационных систем. Проблема начала информационной войны.
9	Типовая стратегия информационной войны. Обобщенный алгоритм информационной войны. Основные аспекты информационной войны. Последствия информационной войны.
10	Защита от несанкционированного доступа (НСД) к информации
11	Классификация автоматизированных систем и требования по защите информации. Документы Гостехкомиссии при Президенте Российской Федерации. Концепции защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности. Требования к информационным системам по обеспечению безопасности информации.
12	Структура системы защиты информации от НСД. Назначение и функции элементов. Направления защиты от НСД. Основные способы НСД. Принципы защиты информации от НСД. Структура системы защиты информации от НСД, назначение и функции элементов
13	Модели управления доступом. Правила разграничения доступа. Мандатная и дискреционная модели управления доступом. Ролевая и атрибутные модели.
14	Основные методы обеспечения информационной безопасности
15	Основные понятия криптографической защиты информации. Определяются предмет и задачи криптографии, формулируются основополагающие определения и требования к криптографическим системам защиты информации, дается историческая справка об основных этапах развития криптографии как науки. Рассматривается пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы.
16	Идентификация и аутентификация. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Пароли, сертификаты и

№ п/п	Тематика лекционных занятий / краткое содержание
	цифровые подписи. Методы аутентификации.
17	Разграничение и контроль доступа к информации. Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации; по способам ее обработки: считать, записать, внести изменения, выполнить команду; по условному номеру терминала; по времени обработки и др. Разделение привилегий на доступ к информации.
18	Технологии межсетевых экранов. Технология межсетевых экранов (МЭ) - защита корпоративных сетей от внешних угроз. Функции МЭ. МЭ способствует реализации политики безопасности, определяет разрешенные службы, типы доступа к ним и является реализацией этой политики в терминах сетевой конфигурации, хостов, маршрутизаторов и других мер защиты.
19	Виртуальные частные сети. Основные понятия и функции виртуальных частных сетей (VPN). Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности VPN.
20	Методы обнаружения вторжений (атак). Краткая история вторжений (атак) на интрасети. Основные понятия. Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений.
21	Компьютерные вирусы и средства антивирусной защиты. Вирусы как угроза информационной безопасности. Средства антивирусной защиты.
22	Стандарты защищенности информации в компьютерных системах
23	Характеристика систем стандартизации в области защиты информации. Информационная безопасность распределенных систем. Европейские критерии безопасности информационных технологий.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ №1 Виды информации и основные методы ее защиты, анализ информационной инфраструктуры государства.
2	ПЗ №2 Основные понятия и общеметодологические принципы информационной безопасности.
3	ПЗ №3 Виды и источники угроз информационной безопасности Российской Федерации.
4	ПЗ №4 Виды и формы применения информационно-технологического оружия.
5	ПЗ №5 Последствия информационной войны.
6	ПЗ №6 1 Причины, виды, каналы утечки и искажения информации, формальная постановка и решение задачи обеспечения информационной безопасности компьютерных систем.

№ п/п	Тематика практических занятий/краткое содержание
7	ПЗ №7 Модели организации кибернетической безопасности.
8	ПЗ №8 Модель избирательного (дискреционного) доступа. Модель ролевого (типизованного) доступа.
9	ПЗ №9 Модель Лендвера-Маклина (MMS).
10	ПЗ №10 Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.
11	ПЗ №11 Программно-аппаратные средства обеспечения информационной безопасности.
12	ПЗ №12 Построение системы разграничения доступа в базе данных на основе ролевой модели.
13	ПЗ №13 Основные понятия криптографической защиты информации. Пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы.
14	ПЗ №14 Классификация систем аутентификации. Электронная подпись и ее применение для контроля целостности программ и данных.
15	ПЗ №15 Виртуальные частные сети. Варианты построения виртуальных защищенных каналов.
16	ПЗ №16 Антивирусные программные комплексы. Восстановление зараженных файлов. Профилактика проникновения «троянских программ».
17	ПЗ №17 Обобщенная архитектура стандартов обеспечения информационной безопасности организации.
18	ПЗ №18 Документы по оценке защищенности автоматизированных систем в РФ.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем, презентаций и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014
2	СР2 Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем, презентаций и др. Защита информации: учебник / В. П. Мель-ников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014
3	СР3 Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем; проведение расчетов и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014 Программно-аппаратные средства защиты информации: учебник для студ. вузов, обуч. по напр. "Информационная безопасность" / В. В. Платонов. - М.: Академия, 2013
4	СР4

№ п/п	Вид самостоятельной работы
	Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем; проведение расчетов и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014 Программно-аппаратные средства защиты информации: учебник для студ. вузов / В. В. Платонов. - М.: Академия, 2013
5	СР5 Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем, презентаций и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014 Оценка уровня информационной безопасности на объекте информатизации: учебное пособие для студ. вузов ж.-д. трансп. / К. А. Паршин. - М.: ФГБОУ "УМЦ ЖДТ", 2015
6	Подготовка к промежуточной аттестации.
7	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Защита информации В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе Академия, , 2014	
2	Программно-аппаратные средства защиты информации К. А. Паршин ФГБОУ "УМЦ ЖДТ" , 2015	
3	Информационная безопасность и защита информации на железнодорожном транспорте: учебник для студ., обуч. по спец. "Информационная безопасность телекоммуникационных систем": в 2 ч. Ч.1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. С. Е. Ададуров [и др.]; под ред. А. А. Корниенко ФГБОУ "УМЦ ЖДТ" , 2014	
4	Основы информационной безопасности Л.М. Груздева Книга Юридический институт МИИТа , 2018	
1	Криптографические методы защиты информации Б. Я. Рябко, А. Н. Фионов Горячая линия-Телеком , 2014	
2	Компьютерные сети и сетевая безопасность В. П. Соловьев, Н. Н. Пуцко МГУПС (МИИТ) , 2014	
3	Информационная безопасность и защита информации на железнодорожном транспорте: учебник для студ., обуч. по спец. "Информационная безопасность телекоммуникационных систем": в 2 ч. Ч.2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. С. Е. Ададуров [и др.]; под ред. А. А. Корниен-ко ФГБОУ "УМЦ ЖДТ" , 2014	

4	Региональная и национальная безопасность А.Б. Логунов Книга ИНФРА-М , 2015	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)
5	Информационное право И.Л. Бачило Книга Издательство Юрайт , 2013	

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

Сайты содержат учебно-методическую документацию, научно-практические публикации, руководящие документы в области информационной безопасности, информационные и аналитические материалы, необходимые для качественного изучения учебной дисциплины. 1. http://citforum.ru — большой учебный сайт по технике и новым технологиям 2. http://www.ict.edu.ru — портал «Информационно-коммуникационные технологии в образовании» 3. http://www.iso27000.ru – портал «Искусство управления информационной безопасностью» 4. http://www.itsec.ru – журнал «Information Security» 5. http://www.inside-zi.ru – журнал «Защита информации» 6. http://www.inside-zi.ru – журнал «Инсайд» 7. http://www.xakep.ru – журнал «Хакер» 8. http://www.compress.ru – журнал «Компьютер пресс» 9. http://www.osp.ru – журнал «Открытые системы» 10. http://www.miit.ru — сайт Московского государственного университета путей сообщения Императора Николая II 11. http://garant.ru – Гарант: законодательство РФ 12. http://www.consultant.ru – Консультант +: законодательство РФ 13. http://www.consultantplus.ru – База данных «Консультант +» 14. http://fstec.ru/ – Федеральная служба по техническому и экспортному контролю (ФСТЭК России) 15. http://www.scrf.gov.ru/ – Совет безопасности РФ 16. http://fsb.ru – ФСБ России Студентам обеспечена возможность свободного доступа к фондам учебно-методической документации и Интернет-ресурсам. Все студенты имеют возможность открытого доступа: - к вузовской ЭБС на платформе Oracle http://miit.ru/portal/page/portal/miit/library/e-catalogue, - к ЭБС Научно-технической библиотеки МИИТа http://library.miit.ru/, - к Российской универсальной научной электронной библиотеке «eLibrary» http://elibrary.ru/, - к электронной библиотеке Book.ru http://book.ru/ - к ЭБС Лань https://e.lanbook.com/, - к ЭБС Юрайт https://biblio-online.ru/, - к ЭБС ibooks.ru http://ibooks.ru/.

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

Установленное лицензионное программное обеспечение.1. Операционная система Microsoft Windows 8 2. Пакет офисных программ Microsoft Office 2013 3. Браузер Internet Explorer 4. Антивирусные программы 5. http://www.consultant.ru – Консультант +: законодательство РФ 6. http://garant.ru – Гарант: законодательство РФ 7. http://fstec.ru/ – ФСТЭК России 8. http://www.iso27000.ru – портал «Искусство управления информационной безопасно-стью»

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

Компьютерный классоборудованный для проведения лекций и практических работ средствами оргтехники, проекторам, персональными компьютерами, объединенными в сеть с выходом в Интернет.

9. Форма промежуточной аттестации:

Зачет в 4 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 «Информационные технологии в юридической деятельности и документационное обеспечение управления» — Груздева Людмила Михайловна

Лист согласования

Заведующий кафедрой УиЗИ	Л.А. Баранов
Заведующий кафедрой ИТЮДиДОУ	С.Л. Лобачев
Председатель учебно-методической комиссии	С.В. Володин