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
09.04.03 Прикладная информатика,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности бизнеса

Направление подготовки: 09.04.03 Прикладная информатика

Направленность (профиль): Прикладная информатика в обеспечении безопасности бизнеса

Форма обучения: Заочная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины является формирование у обучающихся компетенций в соответствии с СУОС «Прикладная информатика» и приобретение ими:

- знаний об основных угрозах бизнес информации, отечественных и международных стандартов в области защиты информации, методах и средствах защиты бизнес информации;
- умений выявлять опасности и угрозы, возникающие в современном информационном обществе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;
- навыков выявления опасностей и угроз информационной безопасности, построения политики информационной безопасности и систем защиты бизнес информации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-54 - Способен обеспечить кибербезопасность в бизнес-процессах при проектировании и эксплуатации информационных систем, управлении проектами в области информационных технологий.

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

Знать:

об основных угрозах бизнес информации, отечественных и международных стандартов в области защиты информации, методах и средствах защиты бизнес информации

Уметь:

выявлять опасности и угрозы, возникающие в современном информационном обществе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

Владеть:

- навыков выявления опасностей и угроз информационной безопасности, построения политики информационной безопасности и систем защиты бизнес информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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. №1
Контактная работа при проведении учебных занятий (всего):	12	12
В том числе:		
Занятия лекционного типа	8	8
Занятия семинарского типа	4	4

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 168 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	Раздел 1. Классификация угроз бизнес информации Внутренние и внешние угрозы. Непреднамеренные ошибки пользователей. Кражи и подлоги. Аварии

№ п/п	Тематика лекционных занятий / краткое содержание
	коммуникаций. Стихийные бедствия. Вредоносное программное обеспечение. Хакеры. Раздел 2. Методология защиты бизнес информации Уровни защиты бизнес информации: правовой, организационный, аппаратно-программный, криптографический Раздел 3. Криптографические методы защиты бизнес информации Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89. Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами. Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция. Раздел 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети. Применение паролей и биометрических средств аутентификации пользователей. Протоколы взаимной проверки подлинности объектов сети. Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI. Обеспечение целостности информации.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Настройка и конфигурирование антивирусного ПО Конфигурирование межсетевого экрана

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	конспектирование отдельных тем учебной литературы, связанных с разделом;
2	Подготовка к промежуточной аттестации.

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

№ п/п	Библиографическое описание	Место доступа

1	Основы информационной безопасности А.А, Варфоломеев Учебное пособие Москва, 2008 , 2008	Библиотека РОАТ
2	Основы информационной безопасности. Галатенко В.А. Учебное пособие М: ИНТУИТ , 2006	библиотека РОАТ

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

Официальный сайт РУТ (МИИТ) (http://miit.ru/)

Электронно-библиотечная система Научно-технической библиотеки МИИТ (http://library.miit.ru/)

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/)

Электронно-библиотечная система РОАТ (http://biblioteka.rgotups.ru/jirbis2/)

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

- Программное обеспечение для выполнения лабораторных работ включает в себя программные продукты общего применения
- Программное обеспечение для демонстрации презентаций и проведения интерактивных занятий: Microsoft Office 2003 и выше.
- Программное обеспечение, необходимое для оформления отчетов и иной документации: Microsoft Office 2003 и выше.

Все необходимые для изучения дисциплины учебно-методические материалы объединены в Учебно-методический комплекс и размещены на сайте университета: http://www.rgotups.ru/.

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

Учебная аудитория для проведения занятий должна соответствовать требованиям охраны труда по освещенности, количеству рабочих (посадочных) мест студентов и качеству учебной (аудиторной) доски, а также соответствовать условиям пожарной безопасности. Освещённость рабочих мест должна соответствовать действующим СНиПам.

Кабинеты должны быть снащены следующим оборудованием, приборами и расходными материалами, обеспечивающими проведение

предусмотренных учебным планом занятий по дисциплине:

-для проведения лекций занятий в помещении должно быть предусмотрено рабочее место студента со стулом, столом, рабочее место преподавателя со стулом, столом, доской (специализированной мебелью), мелом или маркером. -Для организации тематических иллюстраций при проведении лекций (представления презентаций, демонстрационных материалов и видеоматериалов) в аудитории требуется наличие мультимедийного оборудования: стационарный или переносной проектор, стационарный или переносной компьютер (ноутбук), стационарный или переносной экран или интерактивная доска.

-для проведения текущего контроля успеваемости, выполнения контрольной работы, групповых и индивидуальных консультаций в помещении должно быть предусмотрено рабочее место студента со стулом, столом, рабочее место преподавателя со стулом, столом, а также технические средства, служащие для представления учебной информации (доска, стационарный или переносной компьютер (ноутбук) и/или интерактивная доска)

-для организации самостоятельной работы :помещение, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационную среду, в помещении должно быть предусмотрено рабочее место студента со стулом, столом.

- для проведения лабораторных занятий требуется кабинет компьютерных технологий, оборудованный необходимым количеством персональных компьютеров стандартной комплектации (PentiumCore 2DUO 2,53 ГГц/ RAM 1024Mb/HDD 250Gb или аналог) с программным обеспечением согласно п. 9 настоящей рабочей программы:

9. Форма промежуточной аттестации:

Зачет в 1 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

заведующий кафедрой, профессор,
д.н. кафедры «Системы управления
транспортной инфраструктурой» А.В. Горелик

Согласовано:

Заведующий кафедрой СУТИ РОАТ А.В. Горелик

Заведующий кафедрой ПК РОАТ М.В. Маслова

Председатель учебно-методической
комиссии С.Н. Климов