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)

Аудит информационных технологий 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 «Аудит информационных технологий бизнеса» является формирование у обучающихся компетенций в соответствии с самостоятельно установленными образовательными стандартами по направлению подготовки магистров 09.04.03 «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:

- умений 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 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. №3
Контактная работа при проведении учебных занятий (всего):	8	8
В том числе:		
Занятия лекционного типа	4	4
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 100 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 Раздел 1. Классификация угроз бизнес информации Внутренние и внешние угрозы. Непреднамеренные ошибки пользователей. Кражи и подлоги. Аварии коммуникаций. Стихийные бедствия. Вредоносное программное обеспечение. Хакеры. Раздел 2 Раздел 2. Методология оценки защиты бизнес информации Уровни защиты бизнес информации: правовой, организационный, аппаратно-программный, криптографический

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Раздел 1. Классификация угроз бизнес информации Настройка и конфигурирование антивирусного ПО Раздел 2. Методология оценки защиты бизнес информации Конфигурирование межсетевого экрана

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом[осн. 1]
2	Подготовка к промежуточной аттестации.

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

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность Шаньгин В.Ф.	c.e.lanbook.com
1	Моделирование бизнес-процессов: учебник и практикум Долганова О.И., Виноградова Е.В., Лобанова А.М.	c.e.lanbook.com

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

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

2. Электронно-библиотечная система РОАТ – http://biblioteka.rgotups.ru/

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

4. Система дистанционного обучения «Космос» – http://stellus.rgotups.ru/

5. Поисковые системы «Яндекс», «Google» для доступа к тематическим информационным ресурсам

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

7. Электронно-библиотечная система ibooks.ru – http://ibooks.ru /

8. Электронно-библиотечная система «УМЦ» – http://www.umczdt.ru/

9. Электронно-библиотечная система «Intermedia» – http:// www .intermedia-
publishing.ru/

10. Электронно-библиотечная система «BOOK.ru» – http://www.book.ru/

11. Электронно-библиотечная система «ZNANIUM.COM» – http://www.znanium.com/

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

- Программное обеспечение для выполнения практических заданий включает в себя специализированное прикладное программное обеспечение ESET NOD32, а также программные продукты общего применения
- Программное обеспечение для проведения лекций, демонстрации презентаций и ведения интерактивных занятий: Microsoft Office 2003 и выше.
- Программное обеспечение, необходимое для оформления отчетов и иной документации: Microsoft Office 2003 и выше.
- Программное обеспечение для выполнения текущего контроля успеваемости: Браузер Internet Explorer 6.0 и выше.

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

Учебная аудитория должна соответствовать требованиям пожарнойбезопасности и охраны труда по освещенности, количеству рабочих (посадочных) мест студентов.

Учебные лаборатории и кабинеты должны быть оснащены необходимым лабораторным оборудованием, приборами и расходными материалами,

обеспечивающими проведение предусмотренного учебным планом лабораторного практикума (практических занятий) по дисциплине. Освещенность рабочих мест должна соответствовать действующим СНиПам.

Технические требования к оборудованию для осуществления учебного процесса сиспользованием дистанционных образовательных технологий:

колонки, наушники или встроенный динамик (для участия в аудиоконференции);микрофон или гарнитура (для участия в аудиоконференции); веб-камеры (для участия в

видеоконференции);

для ведущего: компьютер с процессором Intel Core 2 Duo от 2 ГГц (или аналог) ивыше, от 2 Гб свободной оперативной памяти.

9. Форма промежуточной аттестации:

Зачет в 3 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»	Горелик Александр Владимирович

Лист согласования

Заведующий кафедрой СУТИ РОАТ	А.В. Горелик
Председатель учебно-методической комиссии	С.Н. Климов