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)

Криптографическая защита бизнес-информации

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 «Криптографическая защита бизнес информации» является формирование у обучающихся компетенций в соответствии с федеральными государственными образовательными стандартами по направлению «Прикладная информатика» и приобретение ими:

- знаний о шифровании с помощью симметричных и ассиметричных ключей;
- умений использовать математические методы в криптографии;
- навыков применения методов криптографической 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:

основы информатизации предприятий и организаций.

Уметь:

- применять различные научные подходы к автоматизации информационных процессов.

Владеть:

- навыками применения научных подходов к информатизации предприятий.

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. №2
Контактная работа при проведении учебных занятий (всего):	16	16
В том числе:		
Занятия лекционного типа	8	8
Занятия семинарского типа	8	8

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 128 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. Математика криптографии. Модульная арифметика, сравнения и матрицы. Алгебраические структуры. Простые числа и уравнения сравнения. Раздел 2. Введение в основы современных шифров с симметричным ключом. Современные блочные шифры. Современные шифры потока. Стандарты шифрования DES и AES. Раздел 3. Криптография с ассиметричным ключом. Криптографические системы RSA. Криптосистемы Рабина и Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. Раздел 4. Некоторые вопросы криптографии. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Системы шифрования DES. Асимметричные криптосистемы. Идентификация, проверки подлинности, цифровая подпись

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделами
2	Выполнение курсовой работы.
3	Подготовка к промежуточной аттестации.

4.4. Примерный перечень тем курсовых работ

Темой является «Криптография с ассиметричным ключом».

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

№ п/п	Библиографическое описание	Место доступа
1	Криптография и безопасность сетей. Б.А. Фороузан М.: Изд-во Бином , 2010	библиотека РОАТ
2	Защита информации в компьютерных системах Ю.В. Романец, П.А. Тимофеев, В.А. Шаньгин М.: Радио и связь , 2007	Библиотка РОАТ.
3	Криптографическая защита информации А.Г. Лихоносов Книга Юридический институт МИИТа , 2011	ИТБ УЛУПС (Абонемент ЮИ)

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 ibooks.ru (http://ibooks.ru/)

Электронно-библиотечная система «УМЦ» (http://www.umczdt.ru/)

Электронно-библиотечная система «Intermedia» (http:// www .intermedia-publishing.ru/)

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 и лабораторных 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:

Курсовая работа во 2 семестре.
Экзамен во 2 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