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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль): Прикладная информатика в информационной сфере

Форма обучения: Заочная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Информационная безопасность» является формирование у обучающихся компетенцийв соответствии

с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС)

по направлению подготовки «Прикладная информатика» и приобретение ими:

- знаний о современных поисковых системах в глобальных компьютерных сетях, об угрозах информационной безопасности, о нормативных правовых документов по информационной безопасности и о методах и средствах обеспечения информационной безопасности;

- умений выявлять угрозы информационной безопасности, использовать нормативные правовые документы по информационной безопасности, использовать методы и средства обеспечения информационной безопасности и проводить обследование организаций;

- навыков определения угроз информационной безопасности, приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения информационной безопасности.

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;

ПК-53 - Способен обеспечить защиту информации в автоматизированных системах в процессе их эксплуатации.

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

Знать:

Знать основные свойства и технологии использования и обработки информации.

Знания: основные математические понятия

Знания: нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий

Уметь:

Умения: Уметь использовать технологии информационных систем

Умения: использовать математические методы в профессиональной деятельности

Умения: использовать нормативно-правовые документы, международные и отечественные

Владеть:

Навыками внедрения информационных технологий

Навыки: основными математическими методами

Навыки: способностью использовать нормативно-правовые документы, международные и отечественные стандарты

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 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	Семестр №4
Контактная работа при проведении учебных занятий (всего):	24	24
В том числе:		
Занятия лекционного типа	8	8
Занятия семинарского типа	16	16

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 192 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. Правовая основа информационной безопасности информационных систем. Предмет, цели и задачи дисциплины “Информационная безопасность”. Основные определения и понятия. Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ. Раздел 2. Информационная безопасность и методология защиты информации в корпоративных системах ФЖТ Классификация информации, циркулирующей в корпоративных системах федерального железнодорожного транспорта (ФЖТ). Информационные ресурсы и информационная инфраструктура сетей ФЖТ как объекты защиты. Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический. Раздел 3. Криптографические методы защиты 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. Аутентификация информации и ЭЦП сообщений. Однонаправленные хэш-функции. Коды проверки подлинности информации. Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов. Раздел 5. Архитектура и методы организации систем защиты информации. Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. Специализированные программно-аппаратные средства защиты информации. Средства и механизмы обеспечения безопасности сетевого оборудования Cisco systems. Серверы доступа (брандмауэры) Cisco ASA5500. Средства обнаружения вторжений IDS 4200. Раздел 6 Дифференцированный зачет Раздел 7 Контрольная работа

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Раздел 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей Настройка правил фильтрации трафика с помощью межсетевого экрана Agnitum OutPost Firewall Для проведения лабораторного практикума требуется необходимое количество комплектов обучающей компьютерной программы (специализированное программное обеспечение) и соответствующая компьютерная техника, предназначенная для работы с указанной программой, позволяющая использовать сетевой прокол TCP/IP и администратор баз данных ODBC32.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	«Шифрование фамилии и полного имени студента методом гаммирования и по алгоритму RSA» Самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом
2	Подготовка к контрольной работе.
3	Подготовка к промежуточной аттестации.

4.4. Примерный перечень тем контрольных работ

«Шифрование фамилии и полного имени студента методом гаммирования и по алгоритму RSA»

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

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность и защита информации В.П.Мельников, С.А.Клейменов, А.М.Петраков М.: Издательский центр "Академия", 2008. - 336 с., , 2008	библиотека РОАТ
2	Комплексная защита информации в корпоративных системах. Шаньгин В.Ф. Учебник М.:Инфра-М, 2010. – 592 с , 2010	Библиотека РОАТ
1	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учебник для вузов ж.-д транспорта Яковлев В.В., Корниенко А.А. Учебник М.: УМК МПС России, 2002.– 328 с , 2002	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 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).

Для осуществления учебного процесса с использованием дистанционныхобразовательных технологий: операционная система Windows, Microsoft Office 2003 и

выше, Браузер Internet Explorer 8.0 и выше с установленным Adobe Flash Player версии10.3 и выше, Adobe Acrobat.

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

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET.

2. Специализированная лекционная аудитория с мультимедиа аппаратурой и инте-рактивной доской.

3. Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET

Для проведения лабораторных занятий: компьютерный класс; кондиционер; компьютеры с минимальными требованиями - Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0

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:

Экзамен в 4 семестре.

10. Оценочные материалы.

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

Авторы:

А.С. Губенко

Согласовано:

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