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
27.03.04 Управление в технических системах,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности

Направление подготовки: 27.03.04 Управление в технических системах

Направленность (профиль): Цифровые технологии управления и обработки данных

Форма обучения: Заочная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 168572
Подписал: заведующий кафедрой Горелик Александр Владимирович
Дата: 22.09.2021

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Основы информационной безопасности» является

формирование у обучающихся компетенций в соответствии с требованиями

самостоятельно утвержденного образовательного стандарта высшего образования (СУОС)

по специальности «Управление в технических системах»

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-51 - Способен обеспечивать информационную безопасность на уровне БД;

ПК-57 - Способен администрировать процесс контроля производительности и управления безопасностью сетевых устройств и программного обеспечения.

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

Знать:

знаний основ в области организационно-правовой и технической защиты информации

Уметь:

умений работать с организационно-правовой документацией по защите информации,

оценивать угрозы объектам защиты информации, выстраивать комплексную систему

защиты информации на предприятии, выявлять и расследовать инциденты

информационной безопасности

Владеть:

навыков расследования компьютерных преступлений

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. №5
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 Раздел 1. Основные теоретические положения в области защиты информации Рассматриваются определение и классификация объектов защиты информации, понятие информации, ее свойства, классификация информации по видам тайн и степеням

№ п/п	Тематика лекционных занятий / краткое содержание
	конфиденциальности, общая характеристика каналов утечки информации, типы угроз информационнной безопасности, а также понятие системы защиты информации Раздел 2 Раздел 2. Правовая защита информации Законодательство в области защиты информации Раздел 3 Раздел 3. Техника защиты информации Рассматриваются основные программно -аппаратные средства защиты информации Раздел 4 Раздел 4. Основы управления инцидентами информационной безопасности Рассматривается понятие инцидентов информационной безопасности, их причины, классификация и план действий при возникновении инцидентов информационной безопасности

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Шифрование на основе схемы Эль-Гамаля Основы управления инцидентами информационной безопасности

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	работа со справочной и специальной литературой, выполнение курсовой работы
2	Подготовка к промежуточной аттестации.

4.4. Примерный перечень тем курсовых работ

«Изучение принципов генерации ключей и процедуры шифрования информации на основе схемы Эль - Гамаля (Elgamal)»

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 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 практических заданий включает в себя программные продукты общего применения: операционная система Windows, Microsoft Office 2003 и выше, Браузер Internet Explorer 8.0 и выше с установленным Adobe Flash Player версии 10.3 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;

2. Специализированная лекционная аудитория с мультимедиа аппаратурой интерактивной доской;

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

4. Для проведения практических 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 с использованием 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) и выше, от 2 Гб свободной оперативной памяти.

9. Форма промежуточной аттестации:

Экзамен в 5 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 «Системы управления транспортной инфраструктурой»	Губенко Инна Михайловна

Лист согласования

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