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 - программа специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Объекты защиты информации

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

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: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

1. Общие сведения о дисциплине (модуле).

Целью изучения дисциплины «Объекты защиты информации» является обеспечение приобретения специалистами знаний о видах и направлениях защиты информации, сущности и свойств объектов, на которые направлена деятельность, называемая защитой информации. Основной целью изучения учебной дисциплины «Объекты защиты информации» является формирование у обучающегося компетенций для следующих видов деятельности: контрольно-аналитическая; эксплуатационная; специализация №8. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): контрольно-аналитическая деятельность: выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты и анализ результатов; проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы; эксплуатационная: установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения; специализация №8 "Информационная безопасность объектов информатизации на базе компьютерных систем": разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации, в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-14 - Способен проводить моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации;

ПК-21 - Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой;

ПК-25 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-26 - Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-27 - Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем;

ПК-28 - Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации.

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

Уметь:

Проводит моделирование автоматизированных систем с целью анализа уязвимостей.

Уметь:

На основании проведенного моделирования определяет эффективность средств и способов защиты информации.

Уметь:

Проводит анализ угроз безопасности информации, обрабатываемой автоматизированными системами высокоскоростного транспорта.

Уметь:

Проводит анализ угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.

Знать:

Знать основные процессы проектирования систем обеспечения информационной безопасности.

Уметь:

Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.

Знать:

Знать основные методы и подходы к анализу защищенности компьютерных систем.

Уметь:

Уметь применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации.

Владеть:

Владеть навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.

Знать:

Знать основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении.

Уметь:

Уметь создавать системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

Владеть:

Владеть навыками создания систем обеспечения информационной безопасности.

Знать:

Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации.

Уметь:

Уметь разрабатывать нормативно правовые акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования.

Владеть:

Владеть навыками разработки нормативной правовой документации

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	Семестр №10
Контактная работа при проведении учебных занятий (всего):	72	72
В том числе:		
Занятия лекционного типа	36	36
Занятия семинарского типа	36	36

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 72 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	Защита информации как деятельность. Виды защиты информации 1. Основные понятия в области техничской защиты информации. Концептуальные основы защиты информации. Система документов по технической защите информации. Органы по технической защите информации в РФ. Лицензирование деятельности в области технической защиты информации. 2. Сертификация средств защиты информации. Аттестация объекта информатизации по требованиям безопасности информации. Классификация угроз и объектов защиты.
2	Цели, направления и объекты защиты информации. Защита информации от непреднамеренного воздействия 1. Объект информатизации. Классификация объектов защиты. Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP. Программно-математическое

№ п/п	Тематика лекционных занятий / краткое содержание
	воздействие. 2. Требования и рекомендации по защите информации. Порядок обеспечения защиты информации в АС.
3	Каналы утечки информации 1. Классификация технических каналов утечки информации. Информационный сигнал и его характеристики. Технические каналы утечки акустической информации. Побочные электромагнитные излучения и наводки. 2. Побочные электромагнитные излучения и наводки. Методы защиты информации от утечки через ПЭМИН.
4	Методы и средства защиты от утечки информации 1. Средства и методы обнаружения технических каналов утечки информации. 2. Мероприятия по выявлению технических каналов утечки информации. 3. Оценка защищенности информации от утечки по ТКУИ.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ1 Определение на компьютере вредоносных программ
2	ПЗ2 Сетевая активность
3	ПЗ3 Текущий контроль по разделам 1 и 2.
4	ПЗ4 Защита от несанкционированного доступа и сетевых хакерских атак
5	ПЗ5 Управление правами пользователей в Windows XP
6	ПЗ6 Работа с реестром
7	ПЗ7 Моделирование технической разведки по исходным данным для объекта информатизации
8	ПЗ8 Текущий контроль по разделам 3 и 4.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Общая и частные цели защиты информации 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Общая и частные цели защиты информации Направления защиты информации и их особенности - из учебной литературы из приведенных источников: [1 с.18-46]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала

№ п/п	Вид самостоятельной работы
2	СР2 Информация как объект правовых отношений 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Информация как объект правовых отношений Классификация носителей информации. Свойства печатных носителей информации - из учебной литературы из приведенных источников:[1 с.55-94]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала 6. Подготовка к текущему контролю ПК 1
3	СР3 Информационный процесс как действие по обработке информации. Взаимосвязь понятий «информационный процесс», «информационная технология», «информационная система» 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Информационный процесс как действие по обработке информации. Взаимосвязь понятий «информационный процесс», «информационная технология», «информационная система» - из учебной литературы из приведенных источников: [1 с.227-244], [доп. 1] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала
4	СР4 Автоматизированная система в защищенном исполнении: основные части, компоненты, функции и задачи. Объект информатизации как особый вид объектов защиты информации. 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Автоматизированная система в защищенном исполнении: основные части, компоненты, функции и задачи. Объект информатизации как особый вид объектов защиты информации - из учебной литературы из приведенных источников:[1 с.227-244], [доп. 1] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала 6. Подготовка к текущему контролю ПК 2
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут , 2006	НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)
1	Безопасность операционных систем и приложений В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007	НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2)

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

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ. http://elibrary.ru/ - научно-электронная библиотека. http://robotosha.ru/ www.chipinfo.ru. http://siblec.ru/ http://autex.ru/ http://www.intuit.ru http://twirpx.com http://habrahabr.ru http://semestr.ru htth://www.cisco.ru Поисковые системы: Yandex, Google, Mail, база научно-технической информации ВИНИТИ РАН.

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

Для проведения лекционных занятийнеобходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.Для проведения практических занятийнеобходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами:

Microsoft Office или Work’11, интегрированная среда разработки программного обеспечения для эиуляции сетевого оборудования OmniGraffle; среда разработки программного обеспечения HTML5 и PHP. Для проведения практических занятий и выполнения курсовой работы необходимо иметь комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ: в области построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше) с поддержкой MPLS; программные продукты Mac OS server, XSan.

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 интерактивной доской. 3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANETДля проведения практических занятий:компьютерный класс; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

9. Форма промежуточной аттестации:

Зачет в 10 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, профессор, д.н. кафедры «Управление и защита информации» В.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин