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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации в интернет и интранет системах

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Дисциплина «Защита информации в интернет и интранет системах» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 « Компьютерная безопасность». Дисциплина «Защита информации в интернет и интранет системах» относится к числу обязательных дисциплин специализации №8. Целью преподавания дисциплины «Защита информации в интернет и интранет системах» является изложение слушателям основных принципов и методов защиты информации, комплексного проектирования и анализа защищенных компьютерных систем КС. Задачами изучения дисциплины являются: изучение основ устройства и принципов функционирования, методологии проектирования и построения защищенных, критериев и методов оценки защищенности КС, средств и методов защиты от несанкционированного доступа (НСД) к информации. Основной целью изучения учебной дисциплины «Защита информации в интернет и интранет системах» является формирование у обучающегося компетенций для организационно-управленческого, эксплуатационного видов деятельности, а также для специализированых профессиональных компетенций специализации №8 "Информационная безопасность объектов информатизации на базе компьютерных систем". Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): Организационно-управленческая деятельность: организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации). Эксплуатационная деятельность: установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем; установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии со специализацией): 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; разработка проектов нормативных правовых актов, руководящих и методических документов предприятия, учреждения,

регламентирующих деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации.

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-20 - Способен подготовить обоснование необходимости защиты информации в автоматизированной системе;

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

ПК-24 - Способен разрабатывать модели угроз, формировать требования по защите 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.

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

Уметь:

Проводит моделирование автоматизированных систем с целью анализа уязвимостей.

Знать:

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

Уметь:

Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта.

Уметь:

Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем

Уметь:

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

Уметь:

Проводит анализ угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.

Знать:

Знать основные формальные модели изолированной программной среды и безопасности информационных потоков.

Уметь:

Уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.

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.

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. №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	Выбор мер защиты информации для их реализации в рамках системы защиты информации в сети интернет и интранет 1. Классификация информационноi? системы по требованиям защиты информации 2. Определение угроз безопасности информации 3. Выбор мер защиты информации для их реализации в рамках ее системы защиты информации
2	Меры защиты информации в сети интернет и интранет 1. Идентификация и аутентификация субъектов доступа и объектов доступа. 2. Управление доступом субъектов доступа к объектам доступа. 3. Ограничение программноi? среды. 4. Защита машинных носителеi? информации. 5. Регистрация событиi? безопасности. 6. Антивирусная защита. 7. Обнаружение (предотвращение)

№ п/п	Тематика лекционных занятий / краткое содержание
	вторжении?. 8. Контроль (анализ) защищенности информации. 9. Обеспечение целостность информации. 10. Обеспечение доступности информации.
3	Меры защиты информации в сети интернет и интранет 1. Обеспечение доступности информации. 2. Защита среды виртуализации. 3. Защита технических средств. 4. Защита средств и систем связи и передачи данных.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ1 Настройка операционной системы Cisco IOS
2	ПЗ2 Защита инфраструктуры маршрутизации
3	ПЗ3 Защита инфраструктуры коммутации
4	ПЗ4 Защита ЛВС от петель на канальном уровне
5	ПЗ5 Защита ЛВС от атак канального уровня
6	ПЗ6 Построение маршрутизируемой ЛВС
7	ПЗ7 Защита сетевой инфраструктуры
8	ПЗ8 Защита периметра сети
9	ПЗ 9 ПК1 - текущ. контроль по разделам 1,2
10	ПЗ10 Криптографическая защита каналов передачи данных
11	ПЗ11 Защита беспроводной ЛВС
12	ПЗ12 Сбор предварительной информации о сети
13	ПЗ13 Идентификация узлов и портов сетевых служб
14	ПЗ14 Идентификация служб и приложений
15	ПЗ15 Идентификация операционных систем
16	ПЗ16 Идентификация уязвимостей сетевых приложений по косвенным признакам
17	ПЗ17 Идентификация уязвимостей на основе тестов

№ п/п	Тематика практических занятий/краткое содержание
18	ПЗ18 ПК2 - текущ. контроль по разделу 3.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Стандарты информационной безопасности в РФ 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Стандарты информационной безопасности в РФ, Административный уровень обеспечения информационной безопасности, Классификация угроз "информационной безопасности» - из учебной литературы из приведенных источников: [1 с.169-204], [2 стр. 3-84] доп. [1 с.5-99]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала
2	СР2 Антивирусные программы 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Антивирусные программы, Профилактика компьютерных вирусов - из учебной литературы из приведенных источников: [1, стр. 3-345] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала 6. Подготовка к промежуточному контролю ПК 1 7. Подготовка к экзамену
3	СР3 Типовые удаленные атаки и их характеристика Сеть MPLS. 1. Подготовка к практическим занятиям 2. Повторение лекционного материала 3. Изучение тем: Типовые удаленные атаки и их характеристика Реализация удаленных угроз в вычислительных сетях Принципы защиты распределенных вычислительных сетей Регистрация и аудит в информационных системах Межсетевое экранирование в интернет Защита КС интеранет с использованием технологии MPLS - из учебной литературы из приведенныхисточников: [1 с. 227-244] , [2 с.36-59], доп.[1, стр. 5-99] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины 5. Конспектирование изученного материала 6. Подготовка к промежуточному контролю ПК 2 7. Оформление курсового проекта
4	Выполнение курсового проекта.
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

выполняется в соответствии со стандартом предприятия в соответствии с методическими указаниями [4] в списке основной литературы. В соответствии с порядковым номером в журнале определяются заданные параметры проекта. Содержание курсовой работы: Введение Структурная схема корпоративной сети с выходом в интернет Модель угроз в корпоративной сети Меры защиты информационных ресурсов в корпоративной сети: - защита авторизации;

- защита доступа; - защита целостности; - защита каналов передачи информации. Заключение

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)
2	Безопасность коммуникационных сетей В.П. Соловьев, А.Е. Шубарев, 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)
3	Методические указания к курсовому проекту	
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

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 9, - 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:

Курсовой проект в 10 семестре.
Экзамен 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»	Алексеев Виктор Михайлович

Лист согласования

Заведующий кафедрой УиЗИ	Л.А. Баранов
Председатель учебно-методической комиссии	С.В. Володин