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:

Знать:

- основные формальные модели изолированной программной среды и безопасности информационных потоков.
- основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении.

Уметь:

- Проводить моделирование автоматизированных систем с целью анализа уязвимостей.
- разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.
- создавать системы обеспечения информационной безопасности

процессов проектирования, создания и модернизации объектов информатизации.

Владеть:

- навыками анализа уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.
- навыками анализа угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.
- 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):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

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 80 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 Рассматриваемые вопросы: - Выбор мер защиты информации для их реализации в рамках системы защиты информации в сети интернет и интранет
2	Информационной системы по требованиям защиты информации Рассматриваемые вопросы: - Классификация информационной системы по требованиям защиты информации
3	Угрозы безопасности информации Рассматриваемые вопросы: - Определение угроз безопасности информации
4	Меры защиты информации Рассматриваемые вопросы: - Выбор мер защиты информации для их реализации в рамках ее системы защиты информации
5	Меры защиты информации в сети интернет и интранет Рассматриваемые вопросы: - основные меры защиты информации в сети интернет и интранет
6	Идентификация и аутентификация субъектов доступа и объектов доступа. Рассматриваемые вопросы: - Идентификация и аутентификация субъектов доступа и объектов доступа.
7	Управление доступом субъектов доступа к объектам доступа. Рассматриваемые вопросы: - Управление доступом субъектов доступа к объектам доступа.
8	Ограничение программной среды. Рассматриваемые вопросы: - Ограничение программной среды.
9	Защита машинных носителей информации. Рассматриваемые вопросы: - Защита машинных носителеи? информации.
10	Регистрация событий безопасности. Рассматриваемые вопросы: - Регистрация событий безопасности.
11	Антивирусная защита. Рассматриваемые вопросы: - Антивирусная защита.
12	Обнаружение (предотвращение) вторжениий. Рассматриваемые вопросы: - Обнаружение (предотвращение) вторжениий.

№ п/п	Тематика лекционных занятий / краткое содержание
13	Контроль (анализ) защищенности информации. Рассматриваемые вопросы: - Контроль (анализ) защищенности информации.
14	Обеспечение целостность информации. Рассматриваемые вопросы: - Обеспечение целостность информации.
15	Обеспечение доступности информации. Рассматриваемые вопросы: - Обеспечение доступности информации.
16	Меры защиты информации в сети интернет и интранет Рассматриваемые вопросы: - Меры защиты информации в сети интернет и интранет
17	Обеспечение доступности информации. Рассматриваемые вопросы: - Обеспечение доступности информации.
18	Защита среды виртуализации. Рассматриваемые вопросы: - Защита среды виртуализации.
19	Защита технических средств. Рассматриваемые вопросы: - Защита технических средств.
20	Защита средств и систем связи и передачи данных. Рассматриваемые вопросы: - Защита средств и систем связи и передачи данных.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Настройка операционной системы Cisco IOS В результате выполнения практического задания студент получает навык настройка операционной системы Cisco IOS
2	Защита инфраструктуры маршрутизации В результате работы на практическом занятии студент определяет основные защита инфраструктуры маршрутизации
3	Защита инфраструктуры коммутации В результате работы на практическом занятии студент определяет защита инфраструктуры коммутации
4	Защита ЛВС В результате работы на практическом занятии студент отрабатывает навык защиты ЛВС от петель на канальном уровне
5	Защита ЛВС от атак канального уровня В результате работы на практическом занятии студент отрабатывает навык защиты ЛВС от атак канального уровня
6	Построение маршрутизируемой ЛВС В результате выполнения практического задания студент учится строить маршрутизируемой ЛВС

№ п/п	Тематика практических занятий/краткое содержание
7	Защита сетевой инфраструктуры В результате выполнения практического задания студент рассматривает защита сетевой инфраструктуры
8	Защита периметра сети В результате выполнения практического задания студент рассматривает защита периметра сети
9	Криптографическая защита каналов передачи данных В результате выполнения практического задания студент учится криптографическая защита каналов передачи данных
10	Защита беспроводной ЛВС В результате выполнения практического задания студент рассматривает защита беспроводной ЛВС
11	Информация о сети В результате выполнения практического задания студент получает навык сбора предварительной информации о сети
12	Идентификация узлов и портов сетевых служб В результате выполнения практического задания студент учится идентификацию узлов и портов сетевых служб
13	ПЗ14 Идентификация служб и приложений
14	ПЗ15 Идентификация операционных систем
15	ПЗ16 Идентификация уязвимостей сетевых приложений по косвенным признакам
16	ПЗ17 Идентификация уязвимостей на основе тестов

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.
6	Выполнение курсового проекта.
7	Подготовка к промежуточной аттестации.
8	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

Курсовая работа на тему «Разработка мер защиты информационных ресурсов в корпоративной сети с выходом в интернет» выполняется в соответствии со стандартом предприятия в соответствии с методическими указаниями 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	НТБ МИИТ
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).

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

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

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office

Work 9,

Интегрированная среда разработки программного обеспечения для эиуляции сетевого оборудования OmniGraffle;

Среда разработки программного обеспечения HTML5 и PHP.

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).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

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» В.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин