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).

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 типами задач профессиональной 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:

- Методы моделирования защищенных автоматизированных систем для анализа их уязвимостей.
- Нормативно-правовую базу и методические документы, регламентирующие необходимость защиты информации в автоматизированных системах.
- Классификацию и характеристику возможных угроз безопасности информации, обрабатываемой в автоматизированных системах.
- Методологию разработки моделей угроз и формирования требований по защите информации для объектов информатизации.
- Основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

Уметь:

- Проводить моделирование автоматизированных систем с целью анализа их уязвимостей и оценки эффективности средств защиты.

- Подготавливать обоснование необходимости защиты информации в автоматизированной системе на основе анализа исходных данных.

- Выявлять и классифицировать возможные угрозы безопасности информации, обрабатываемой в автоматизированной системе.

- Разрабатывать модели угроз и модели нарушителя для компьютерных систем и объектов информатизации.

- Участвовать в создании систем обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

Владеть:

- Навыками анализа уязвимостей и выбора необходимых средств защиты информации для автоматизированных систем.

- Методами сбора и анализа исходных данных для обоснования необходимости защиты информации.

- Навыками анализа угроз безопасности информации, обрабатываемой автоматизированными системами.

- Методиками разработки моделей угроз и формирования требований по защите информации.

- Навыками создания и интеграции систем обеспечения информационной безопасности в процессы проектирования и модернизации.

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):	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. Меры защиты информации Рассматриваемые вопросы: - Определение угроз безопасности информации - Выбор мер защиты информации для их реализации в рамках ее системы защиты информации
4	Меры защиты информации в сети интернет и интранет Рассматриваемые вопросы: - основные меры защиты информации в сети интернет и интранет
5	Идентификация и аутентификация субъектов доступа и объектов доступа. Рассматриваемые вопросы: - Идентификация и аутентификация субъектов доступа и объектов доступа.
6	Управление доступом субъектов доступа к объектам доступа. Рассматриваемые вопросы: - Управление доступом субъектов доступа к объектам доступа.
7	Ограничение программной среды. Защита машинных носителей информации. Рассматриваемые вопросы: - Ограничение программной среды. - Защита машинных носителеи? информации.

№ п/п	Тематика лекционных занятий / краткое содержание
8	Регистрация событий безопасности. Рассматриваемые вопросы: - Регистрация событий безопасности.
9	Антивирусная защита. Обнаружение (предотвращение) вторжениий. Рассматриваемые вопросы: - Антивирусная защита. - Обнаружение (предотвращение) вторжениий.
10	Контроль (анализ) защищенности информации. Рассматриваемые вопросы: - Контроль (анализ) защищенности информации.
11	Обеспечение целостность информации. Рассматриваемые вопросы: - Обеспечение целостность информации.
12	Обеспечение доступности информации. Рассматриваемые вопросы: - Обеспечение доступности информации.
13	Меры защиты информации в сети интернет и интранет Рассматриваемые вопросы: - Меры защиты информации в сети интернет и интранет
14	Обеспечение доступности информации. Рассматриваемые вопросы: - Обеспечение доступности информации.
15	Защита среды виртуализации. Защита технических средств. Рассматриваемые вопросы: - Защита среды виртуализации. - Защита технических средств.
16	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

№ п/п	Тематика практических занятий/краткое содержание
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
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	Организация VPN на сетевом оборудовании В результате работы студент изучает принципы организации VPN-туннелей (IPSec, GRE) на сетевом оборудовании Cisco.
14	Настройка межсетевого экранирования В результате работы студент получает навык настройки списков доступа (ACL) для фильтрации трафика и обеспечения периметровой защиты сети.
15	Мониторинг и аудит событий безопасности В результате работы студент изучает настройку систем логирования и мониторинга событий безопасности на сетевых устройствах.
16	Защита инфраструктуры коммутации В результате работы на практическом занятии студент изучает методы защиты инфраструктуры коммутации (Port Security, DHCP Snooping, Dynamic ARP Inspection).

4.3. Самостоятельная работа обучающихся.

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

4.4. Примерный перечень тем курсовых проектов

1. Разработка модели угроз и нарушителя для корпоративной сети предприятия.

2. Проектирование системы защиты информации для сегмента сети с выходом в Интернет.

3. Анализ уязвимостей и выбор средств защиты для беспроводного сегмента сети.

4. Разработка политики безопасности для интранет-портала организации.

5. Проектирование системы защиты каналов передачи данных с использованием VPN.

6. Обеспечение безопасности межсетевого взаимодействия при подключении филиалов.

7. Разработка мер защиты от атак канального уровня в локальной вычислительной сети.

8. Проектирование системы идентификации, аутентификации и авторизации для корпоративной сети.

9. Анализ эффективности антивирусной защиты в сегменте корпоративной сети.

10. Разработка системы мониторинга и регистрации событий безопасности в сети.

11. Обеспечение защиты информации при использовании облачных сервисов в корпоративной сети.

12. Проектирование системы защиты для сегмента сети, обрабатывающего конфиденциальную информацию.

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

№ п/п	Библиографическое описание	Место доступа
1	Защита информации Груздева Л. М. Учебное пособие М.: Российский университет транспорта, - 144 с. - ISBN 978-5-7876-0326-2 , 2019	https://reader.lanbook.com/book/188703
2	Техническая защита информации Раков А. С., Маслов О. Н., Губарева О. Ю., Почепцов А. О., Гуреев В. О. Учебное пособие Поволжский государственный университет телекоммуникаций и информатики, - 96 с. , 2020	https://reader.lanbook.com/book/255575

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