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)

Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих.

Студенты должны научиться применять современные средства защиты информации предоставляемые сетевым оборудованием, являющимся самым уязвимым местом при попытке несанкционированного доступа.

Основными задачами дисциплины являются:

• Ознакомление с основными терминами и определениями.

• Ознакомление с основными типами угроз и атак.

• Изучение механизмов защиты административного интерфейса и разграничения прав доступа.

• Изучение технологии AAA. • Изучение способов защиты информации в сетях.

• Изучение принципов построения виртуальных частных сетей.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): научно-исследовательская; контрольно-аналитическая; специализация №8.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): Научно-исследовательская деятельность: сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности; изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте; подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований. Контрольно-аналитическая деятельность: предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей; применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты; подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

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-15 - Способен принимать участие в разработке проектных решений по защите информации в автоматизированных системах;

ПК-17 - Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации;

ПК-18 - Способен принимать участие в разработке архитектуры системы защиты информации автоматизированной системы;

ПК-22 - Способен проводить тестирование систем защиты информации автоматизированных систем;

ПК-23 - Способен участвовать в разработке эксплуатационной документации на системы защиты информации автоматизированных систем;

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:

Участвует в разработке проектных решений по защите информации в автоматизированных системах высокоскоростного транспорта.

Уметь:

Участвует в разработке проектных решений по защите информации в беспилотных автоматизированных системах.

Уметь:

Проводит сравнительный анализ программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

Знать:

Делает обоснованный выбор программно-аппаратных средств защиты информации.

Уметь:

Участвует в разработке архитектуры системы защиты информации автоматизированных систем высокоскоростного транспорта.

Уметь:

Участвует в разработке архитектуры системы защиты информации беспилотных автоматизированных систем.

Уметь:

Проводит индивидуальное тестирование систем защиты информации в блоке автоматизированных систем.

Уметь:

Участвует в разработке эксплуатационной документации системы защиты информации в автоматизированных системах высокоскоростного транспорта.

Уметь:

Участвует в разработке эксплуатационной документации на системы защиты информации в беспилотных автоматизированных системах.

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 1
Контактная работа при проведении учебных занятий (всего):	90	90
В том числе:		
Занятия лекционного типа	54	54
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 54 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	Понятие защиты информации. Рассматриваемые вопросы: - цель обеспечения информационной безопасности; - виды контроля безопасности.
2	Составляющие информационной безопасности. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- конфиденциальность; - целостность; - доступность; - принципы внедрения систем информационной безопасности.
3	Средства защиты информационной безопасности. Рассматриваемые вопросы: - классификация угроз информационной безопасности; - виды средств защиты информации; - примеры средств защиты информации.
4	ГОСТ Р 50922-2006 Защита информации и виды защиты. Рассматриваемые вопросы: - виды защиты информации; - способы защиты информации; - техника защиты информации; - способы оценки соответствия требованиям защиты информации; - эффективность защиты информации.
5	Политика зашиты. Рассматриваемые вопросы: - цели политики защиты; - задачи политики защиты; - основные требования к политике защиты; - содержание политики защиты.
6	Работа с персоналом организации в рамках политики защиты. Рассматриваемые вопросы: - организация работы по контролю состояния защиты конфиденциальной информации; - организация работы с персоналом предприятия, допущенного к конфиденциальной информации.
7	Угрозы информационной безопасности. Рассматриваемые вопросы: - виды угроз информационной безопасности; - источники угроз информационной безопасности.
8	Опасные влияния на информационные системы. Рассматриваемые вопросы: - реализация сценариев угроз информационной безопасности; - несанкционированный доступ; - непосредственные и непрямые угрозы информационной безопасности; - методы организации защиты информации.
9	Компьютерные вирусы. Рассматриваемые вопросы: - классификация компьютерных вирусов; - методы защиты от компьютерных вирусов; - вредоносное воздействие компьютерных вирусов.
10	Защита сети. Рассматриваемые вопросы: - направления защиты сети; - уязвимые места, через которые может быть выполнен несанкционированный доступ к сетевому оборудованию; - требования для защиты административного интерфейса сетевого оборудования; - настройка контекстных списков доступа.
11	Аутентификация, авторизация, учет. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- необходимость; - примеры протоколов; - основные решения; - настройка удаленного доступа для администрирования сетевого оборудования.
12	Интеграция систем защиты информации от несанкционированного доступа с контролем доступа и видеонаблюдением. Рассматриваемые вопросы: - достоинства интеграции систем защиты информации от несанкционированного доступа с контролем доступа и видеонаблюдением; - объединение систем на нескольких уровнях; - схема информационных потоков; - пример сценария.
13	Управление правами доступа к корпоративным файловым информационным ресурсам. Рассматриваемые вопросы: - основные понятия и определения; - сфера применения; - основные принципы управления правами доступа; - модель разграничения доступа; - правила именования групп доступа пользователей; - процессы управления доступом к файловым информационным ресурсам.
14	Защита информации в критической информационной инфраструктуре. Рассматриваемые вопросы: - принадлежность объекта информатизации к критической информационной инфраструктуре; - возможности средств защиты сетевого взаимодействия между объектами в критической информационной инфраструктуре; - аппаратная защита данных в объектах критической информационной инфраструктуры; - требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
15	Доверенная вычислительная среда как средство защиты информации. Рассматриваемые вопросы: - доверенная загрузка; - условия обеспечения доверенной загрузки операционной системы; - доверенная вычислительная система; - условия доверенности компьютера и доверенного сетевого соединения; - доверенный сеанс связи; - особенности построения защищённых распределенных информационных систем.
16	Сетевая защита на базе межсетевых экранов. Рассматриваемые вопросы: - принципы сетевой защиты на базе межсетевых экранов; - формирование политики межсетевого взаимодействия; - политика доступа к сетевым сервисам; - политика работы межсетевого экрана; - выполняемые функции и составные элементы анализа; - основные схемы подключения межсетевых экранов.
17	Система удаленного централизованного управления средствами защиты информации от несанкционированного доступа. Рассматриваемые вопросы: - назначение и основные элементы; - функции системы;

№ п/п	Тематика лекционных занятий / краткое содержание
	- функции системы удаленного централизованного управления средствами защиты информации от несанкционированного доступа; - состав ролей системы удаленного централизованного управления средствами защиты информации от несанкционированного доступа.
18	Защита информационной системы персональных данных. Рассматриваемые вопросы: - требования регуляторов по защите персональных данных и требования к информационной системе персональных данных для различных уровней защиты; - сетевая инфраструктура информационной системы персональных данных и меры ее защиты; - оптимизация сетевой инфраструктуры; - средства защиты информации от несанкционированного доступа.
19	Безопасность Web-приложений. Рассматриваемые вопросы: - угрозы информационной безопасности при использовании Web-сервера; - методы и средства защиты информационной безопасности для Web-приложений; - угрозы и уязвимости информационной безопасности, возникающие в Web-среде; - меры по ликвидации угроз и уязвимостей информационной безопасности, возникающих в Web-среде.
20	Применение криптографии и средств криптографической защиты информации. Рассматриваемые вопросы: - средства криптографической защиты информации; - принципы шифрования; - применение криптографии и средств криптографической защиты информации.
21	Электронная цифровая подпись. Рассматриваемые вопросы: - принцип использования электронной цифровой подписи; - алгоритмы электронной цифровой подписи; - особенности применения электронной цифровой подписи.
22	Носители ключевой информации как средства безопасности. Рассматриваемые вопросы: - безопасность средств хранения ключевой информации; - виды носителей ключевой информации; - контроль среды доступа к носителю ключевой информации; - «идеальный токен»: принципы функционирования.
23	Построение виртуальных частных сетей (VPN). Рассматриваемые вопросы: - необходимость виртуальной частной сети; - реализация виртуальных частных сетей; - протоколы виртуальных частных сетей.
24	Вопросы проектирования информационных систем. Рассматриваемые вопросы: - основные подготовительные вопросы при проектировании информационных систем; - стадии разработки информационной системы; - формирование требований к проектируемой информационной системе; - показатели качества функционирования информационной системы.
25	Защита информации в АСУ ТП. Рассматриваемые вопросы: - факторы, влияющие на информационную безопасность современных АСУ ТП; - особенности обследования и аудита; - цели и концепции информационной безопасности в АСУ ТП.

№ п/п	Тематика лекционных занятий / краткое содержание
26	Реализация законодательства РФ о безопасности критической информационной инфраструктуры (КИИ). Рассматриваемые вопросы: - основные этапы реализации 187-ФЗ от 26.07.2017 г.; - средства обеспечения безопасности объектов КИИ; - угрозы информационной безопасности и механизмы их предупреждения.
27	Особенности обеспечения информационной безопасности в современных условиях. Рассматриваемые вопросы: - основные инструменты реализации угроз; - ключевые цели информационной инфраструктуры для злоумышленников; - угрозы информационной безопасности и меры защиты.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Защита информации Основные термины и определения. Рассматриваются основные термины и определения в соответствии с ГОСТ Р 50922-2006. Рассматриваются основные направления действия системы защиты информации и принципы ее организации.
2	Политика защиты Сетевая безопасность. Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты. Анализ угроз безопасности. Описываются типы угроз и общие рекомендации по борьбе с ними. Вирусы. Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие.
3	Защита сети Защита административного доступа к сетевым устройствам. Рассматриваются вопросы защиты доступа к административным интерфейсам. Описываются методы усиления парольной защиты и разделения уровней привилегий. Защита связи между маршрутизаторами. Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации, ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика. Технология защиты AAA. Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования.
4	Защита сетевых соединений Модели обороны. Рассматриваются существующие модели обороны, их преимущества и недостатки. Защита периметра сети. Описывается зонная архитектура защиты сети и ее компоненты. Контроль сервисов TCP/IP. Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов. Контроль доступа. Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, CBAC и их конфигурация, а также настройка средств защиты от синхронных атак.
5	Шифрование Механизмы шифрования. Рассматриваются различные варианты построения систем шифрования и их свойства. Блочное шифрование и цифровая подпись. Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES. AES, ГОСТ 28147, RSA RC5. Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA. Шифрование на сетевом уровне. Приводится обзор задач и средств шифрования на сетевом уровне.

№ п/п	Тематика практических занятий/краткое содержание
6	Построение виртуальных частных сетей с использованием IPSec Обзор технологии виртуальных частных сетей. Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки. Механизмы IPSec. Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE. Настройка IPSec VPN. Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Защита информации Основные термины и определения. Рассматриваются основные термины и определения в соответствии с ГОСТ Р 50922-2006. Рассматриваются основные направления действия системы защиты информации и принципы ее организации.
2	Политика защиты Сетевая безопасность. Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты. Анализ угроз безопасности. Описываются типы угроз и общие рекомендации по борьбе с ними. Вирусы. Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие.
3	Защита сети Защита административного доступа к сетевым устройствам. Рассматриваются вопросы защиты доступа к административным интерфейсам. Описываются методы усиления парольной защиты и разделения уровней привилегий. Защита связи между маршрутизаторами. Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации, ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика. Технология защиты AAA. Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования.
4	Защита сетевых соединений Модели обороны. Рассматриваются существующие модели обороны, их преимущества и недостатки. Защита периметра сети. Описывается зонная архитектура защиты сети и ее компоненты. Контроль сервисов TCP/IP. Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов. Контроль доступа. Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, CBAC и их конфигурация, а также настройка средств защиты от синхронных атак.
5	Шифрование Механизмы шифрования. Рассматриваются различные варианты построения систем шифрования и их свойства. Блочное шифрование и цифровая подпись. Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES. AES, ГОСТ 28147, RSA RC5. Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA. Шифрование на сетевом уровне. Приводится обзор задач и средств шифрования на сетевом уровне.
6	Построение виртуальных частных сетей с использованием IPSec Обзор технологии виртуальных частных сетей. Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки. Механизмы IPSec. Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE. Настройка IPSec VPN. Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.
7	Подготовка к промежуточной аттестации.

8	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Основы построения опорных сетей ISP. Учебное пособие. Желенков Б.В. МИИТ , 2009	
2	Проектирование кампусных сетей Я.М. Голдовский Книга 2009	
1	Криптографическая защита компьютерной информации. Методические указания к лабораторным работам. Голдовский Я.М. Желенков Б.В. МИИТ , 2013	

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

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Тематический форум по информационным технологиям http://habrahabr.ru/

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

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой.

Компьютер должен быть обеспечен лицензионными программными продуктами: Foxit Reader/Acrobat Reader Microsoft Office (Power Point) Установлен мультимедийный курс лекций.

Для проведения практических занятий необходимы персональные компьютеры с рабочими местами.

Компьютер должен быть обеспечен лицензионными программными продуктами: Foxit Reader/Acrobat Reader Microsoft Office (Word). На рабочие места должны быть установлены программные разработки кафедры «Вычислительные системы и сети»: Обучающая система «netlab»

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения аудиторных занятий требуется специализированная лекционная аудитория с мультимедиа аппаратурой.Для проведения лабораторных работ: компьютеры с предустановленным Microsoft Windows не ниже Windows XP и процессором не ниже Pentium 4.

- маршрутизаторы Cisco;
- коммутаторы Cisco;
- соединительные кабели различных типов

9. Форма промежуточной аттестации:

Экзамен в 10 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, доцент, к.н. кафедры
«Управление и защита информации» С.Е. Иконников

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин