

**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

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: 01.06.2024

## 1. Общие сведения о дисциплине (модуле).

Целями освоения дисциплины (модуля) являются:

- ознакомление с основными типами угроз и атак;
- изучение механизмов защиты административного интерфейса и разграничения прав доступа;
- изучение технологии и принципов AAA;
- изучение способов защиты информации в сетях;
- изучение принципов построения виртуальных частных сетей.

Основные задачи дисциплины (модуля) следующие:

- поиска и проверки новых технических и программных решений по совершенствованию систем и средств информационной безопасности;
- разработки планов, программ и методик проведения исследований уровня защищенности объектов информатизации, анализ их результатов.

## 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:

**Знать:**

- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, основы системного администрирования;
- устройство и функционирование современных информационных систем;
- современные стандарты информационного взаимодействия систем;
- программные средства и платформы инфраструктуры информационных технологий организаций;
- основы информационной безопасности организации.

**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;
- устанавливать права доступа к файлам и папкам;
- анализировать входные данные.

**Владеть:**

- навыками разработки нормативной правовой документации с сфере информационной безопасности;
- основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации;
- определением базовых элементов конфигурации информационных систем;
- планированием аудитов конфигураций информационных систем.

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):	96	96
В том числе:		
Занятия лекционного типа	48	48
Занятия семинарского типа	48	48

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 48 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. Средства защиты информационной безопасности. Рассматриваемые вопросы: - конфиденциальность;

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> <li>- целостность;</li> <li>- доступность;</li> <li>- принципы внедрения систем информационной безопасности;</li> <li>- классификация угроз информационной безопасности;</li> <li>- виды средств защиты информации;</li> <li>- примеры средств защиты информации.</li> </ul>
3	<p>ГОСТ Р 50922-2006 Защита информации и виды защиты.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- виды защиты информации;</li> <li>- способы защиты информации;</li> <li>- техника защиты информации;</li> <li>- способы оценки соответствия требованиям защиты информации;</li> <li>- эффективность защиты информации.</li> </ul>
4	<p>Политика защиты.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- цели политики защиты;</li> <li>- задачи политики защиты;</li> <li>- основные требования к политике защиты;</li> <li>- содержание политики защиты.</li> </ul>
5	<p>Работа с персоналом организации в рамках политики защиты.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- организация работы по контролю состояния защиты конфиденциальной информации;</li> <li>- организация работы с персоналом предприятия, допущенного к конфиденциальной информации.</li> </ul>
6	<p>Угрозы информационной безопасности.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- виды угроз информационной безопасности;</li> <li>- источники угроз информационной безопасности.</li> </ul>
7	<p>Опасные влияния на информационные системы.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- реализация сценариев угроз информационной безопасности;</li> <li>- несанкционированный доступ;</li> <li>- непосредственные и не прямые угрозы информационной безопасности;</li> <li>- методы организации защиты информации.</li> </ul>
8	<p>Компьютерные вирусы.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- классификация компьютерных вирусов;</li> <li>- методы защиты от компьютерных вирусов;</li> <li>- вредоносное воздействие компьютерных вирусов.</li> </ul>
9	<p>Защита сети.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- направления защиты сети;</li> <li>- уязвимые места, через которые может быть выполнен несанкционированный доступ к сетевому оборудованию;</li> <li>- требования для защиты административного интерфейса сетевого оборудования;</li> <li>- настройка контекстных списков доступа.</li> </ul>
10	<p>Аутентификация, авторизация, учет.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- необходимость;</li> <li>- примеры протоколов;</li> <li>- основные решения;</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
	- настройка удаленного доступа для администрирования сетевого оборудования.
11	<p>Интеграция систем защиты информации от несанкционированного доступа с контролем доступа и видеонаблюдением.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- достоинства интеграции систем защиты информации от несанкционированного доступа с контролем доступа и видеонаблюдением;</li> <li>- объединение систем на нескольких уровнях;</li> <li>- схема информационных потоков;</li> <li>- пример сценария.</li> </ul>
12	<p>Управление правами доступа к корпоративным файловым информационным ресурсам.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- основные понятия и определения;</li> <li>- сфера применения;</li> <li>- основные принципы управления правами доступа;</li> <li>- модель разграничения доступа;</li> <li>- правила именования групп доступа пользователей;</li> <li>- процессы управления доступом к файловым информационным ресурсам.</li> </ul>
13	<p>Защита информации в критической информационной инфраструктуре.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- принадлежность объекта информатизации к критической информационной инфраструктуре;</li> <li>- возможности средств защиты сетевого взаимодействия между объектами в критической информационной инфраструктуре;</li> <li>- аппаратная защита данных в объектах критической информационной инфраструктуры;</li> <li>- требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.</li> </ul>
14	<p>Доверенная вычислительная среда как средство защиты информации.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- доверенная загрузка;</li> <li>- условия обеспечения доверенной загрузки операционной системы;</li> <li>- доверенная вычислительная система;</li> <li>- условия доверенности компьютера и доверенного сетевого соединения;</li> <li>- доверенный сеанс связи;</li> <li>- особенности построения защищённых распределенных информационных систем.</li> </ul>
15	<p>Сетевая защита на базе межсетевых экранов.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- принципы сетевой защиты на базе межсетевых экранов;</li> <li>- формирование политики межсетевого взаимодействия;</li> <li>- политика доступа к сетевым сервисам;</li> <li>- политика работы межсетевого экрана;</li> <li>- выполняемые функции и составные элементы анализа;</li> <li>- основные схемы подключения межсетевых экранов.</li> </ul>
16	<p>Система удаленного централизованного управления средствами защиты информации от несанкционированного доступа.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- назначение и основные элементы;</li> <li>- функции системы;</li> <li>- функции системы удаленного централизованного управления средствами защиты информации от несанкционированного доступа;</li> <li>- состав ролей системы удаленного централизованного управления средствами защиты информации от несанкционированного доступа.</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
17	<p>Защита информационной системы персональных данных.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- требования регуляторов по защите персональных данных и требования к информационной системе персональных данных для различных уровней защиты;</li> <li>- сетевая инфраструктура информационной системы персональных данных и меры ее защиты;</li> <li>- оптимизация сетевой инфраструктуры;</li> <li>- средства защиты информации от несанкционированного доступа.</li> </ul>
18	<p>Безопасность Web-приложений.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- угрозы информационной безопасности при использовании Web-сервера;</li> <li>- методы и средства защиты информационной безопасности для Web-приложений;</li> <li>- угрозы и уязвимости информационной безопасности, возникающие в Web-среде;</li> <li>- меры по ликвидации угроз и уязвимостей информационной безопасности, возникающих в Web-среде.</li> </ul>
19	<p>Применение криптографии и средств криптографической защиты информации.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- средства криптографической защиты информации;</li> <li>- принципы шифрования;</li> <li>- применение криптографии и средств криптографической защиты информации.</li> </ul>
20	<p>Электронная цифровая подпись.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- принцип использования электронной цифровой подписи;</li> <li>- алгоритмы электронной цифровой подписи;</li> <li>- особенности применения электронной цифровой подписи.</li> </ul>
21	<p>Носители ключевой информации как средства безопасности.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- безопасность средств хранения ключевой информации;</li> <li>- виды носителей ключевой информации;</li> <li>- контроль среды доступа к носителю ключевой информации;</li> <li>- «идеальный токен»: принципы функционирования.</li> </ul>
22	<p>Построение виртуальных частных сетей (VPN).</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- необходимость виртуальной частной сети;</li> <li>- реализация виртуальных частных сетей;</li> <li>- протоколы виртуальных частных сетей.</li> </ul>
23	<p>Защита информации в АСУ ТП.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- факторы, влияющие на информационную безопасность современных АСУ ТП;</li> <li>- особенности обследования и аудита;</li> <li>- цели и концепции информационной безопасности в АСУ ТП;</li> <li>- основные этапы реализации 187-ФЗ от 26.07.2017 г.;</li> <li>- средства обеспечения безопасности объектов критической информационной инфраструктуры;</li> <li>- угрозы информационной безопасности и механизмы их предупреждения.</li> </ul>
24	<p>Особенности обеспечения информационной безопасности в современных условиях.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- основные инструменты реализации угроз;</li> <li>- ключевые цели информационной инфраструктуры для злоумышленников;</li> <li>- угрозы информационной безопасности и меры защиты.</li> </ul>

#### 4.2. Занятия семинарского типа.

## Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Организация работы с персоналом предприятия, допущенного к конфиденциальной информации В результате работы на практическом занятии студент отрабатывает навык овладение основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации, основами системного администрирования.
2	Анализ угроз безопасности в локальных сетях В результате работы на практическом занятии студент отрабатывает навык овладение основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации, основами системного администрирования.
3	Практическая реализация политики защиты В результате работы на практическом занятии студент отрабатывает навык овладение основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации, основами системного администрирования.
4	Управление правами доступа к корпоративным информационным ресурсам В результате работы на практическом занятии студент получает навык овладение основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации, основами системного администрирования; установка прав доступа к файлам и папкам.
5	Построение централизованной защищенной системы В результате работы на практическом занятии студент получает навык овладение основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации, основами системного администрирования; установка прав доступа к файлам и папкам; анализ входных данных.

### 4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом и изучение литературы по дисциплине
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.
4	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	<a href="http://library.mii.ru/">http://library.mii.ru/</a> УДК 681.3 Ж51
2	Проектирование кампусных сетей Я.М. Голдовский Книга 2009	
3	Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга	ИТБ УЛУПС (Абонемент ЮИ); ИТБ

	Издательский центр "Академия" , 2011	УЛУПС (ЧЗІ ЮИ)
4	Защита программ и данных В.Г. Проскурин Издательский центр "Академия" , 2011	НТБ МИИТ
5	ГОСТ Р 50922-96 Защита информации. Основные	<a href="http://standartgost.ru/">http://standartgost.ru/</a>
1	Криптографическая защита компьютерной информации. Методические указания к лабораторным работам. Голдовский Я.М. Желенков Б.В. МИИТ , 2013	<a href="http://library.miit.ru/">http://library.miit.ru/</a> УДК 681.3 Г60

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) (<http://ibooks.ru/>).

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).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

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

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).

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

Для проведения практических занятий:

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  
Председатель учебно-методической  
комиссии

Л.А. Баранов

С.В. Володин