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)

Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Основной целью изучения дисциплины «Обеспечение информационной безопасности АСУ ТП» является формирование у обучающегося компетенций для следующих видов деятельности: - проектная; - организационно-управленческая.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): Проектная деятельность: - разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов; - разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием. Организационно-управленческая деятельность: - осуществление правового, организационного и технического обеспечения защиты информации; - организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации); Специализация №8 "Информационная безопасность объектов информатизации на базе компьютерных систем": - 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. Дисциплина «Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении» имеет целью ознакомление слушателей с нормативными и организационными документами, доктринами, стандартами ФСБ и ФСТЭК. Дисциплина обеспечивает приобретение знаний и умений в области защиты информации по утечке в различных каналах связи и несанкционированному доступу к ней.

Задача дисциплины «Обеспечение информационной безопасности АСУ ТП» – получение основополагающих знаний о методах обеспечения безопасности информации на различных обьектах защет руководящих и нормативных документов, а так же внутренних документов организации, и о каналах утечки защищаемой информации.

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

ПК-16 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем;

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

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-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 разработки, расчета и проектирования систем и средств автоматизации и управления

Уметь:

- Разрабатывать и формулировать техническое задание для проектирования автоматизированной системы управления и (или) её

составляющих.

- Выполнять документирование и моделирование бизнес-процессов и технологических процессов объекта автоматизации.

Владеть:

- навыками анализа существующих разработок систем и средств автоматизации и управления; формулирует критерии качества; обобщает выводы.

- навыками анализа уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта.

- навыками анализа уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных 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	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	Введение Рассматриваемые вопросы: - Правовые основы обеспечения защиты информации.
2	Утечка информации по техническим каналам Рассматриваемые вопросы: - Технические каналы утечки информации. - Технические средства минимизации ущерба от инцидентов.
3	Информационные технологии. Рассматриваемые вопросы: - Угрозы безопасности информационных технологий. - Виды мер и основные принципы обеспечения безопасности информационных технологий. - Правовые основы обеспечения безопасности информационных технологий. - Государственная система защиты информации.
4	Меры и средства защиты информации. Рассматриваемые вопросы: - Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. - Организационная структура системы обеспечения безопасности информационных технологий. - Распределение функций. - Система нормативно-методических и организационно-распорядительных документов организации по обеспечению безопасности информационных технологий.
5	Аппаратно-программные средства защиты информации от несанкционированного доступа. Рассматриваемые вопросы: - Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа.
6	Безопасность в компьютерных системах и сетях Рассматриваемые вопросы: - Проблемы обеспечения безопасности в компьютерных системах и сетях. - Назначение, возможности, и основные защитные механизмы межсетевых экранов. - Виртуальные частные сети. - Обнаружение и устранение уязвимостей. - Возможности сканеров безопасности. - Анализ содержимого почтового и WEB-трафика (CONTENT SECURITY).
7	Аудит информационной безопасности Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- События безопасности, аудит. - Мониторинг событий безопасности. - Стандартны и критерии проведения аудита информационной безопасности. 3. - Методология аудита информационной безопасности. Организация процесса аудита.
8	Техническая защита информации Рассматриваемые вопросы: - Основные приборы и оборудование, применяемое для выявления технических каналов утечки информации. - Основы организации и обеспечения работ по технической защите информации. - Технические средства защиты информации и организация работ по защите информации.
9	Компьютерные инциденты Рассматриваемые вопросы: - Понятие о компьютерных инцидентах. - Минимизация ущерба, наносимого инцидентом. - Юридические предпосылки для расследования инцидентов и минимизации ущерба. - Расследование инцидентов в Российской Федерации и за рубежом. - Некоторые средства контроля коммуникаций и средств ЭВТ. - Действия в случае возникновения инцидента. - Изъятие и исследование компьютерной техники и носителей информации.
10	Методы аудирования. Рассматриваемые вопросы: - Основные понятия в области безопасности информационных технологий. - Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях. - Ответственность за нарушения. - Порядок работы с носителями ключевой информации. - Инструкции по организации паролей и антивирусной защиты. - Аудит информационной безопасности компаний: общие понятия и определения.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Вводное занятие. В результате выполнения работы студент изучает особенности техники безопасности в компьютерном классе.
2	Практическое занятие №2 В результате студент докладывает по теме «Технические каналы утечки информации», «Технические средства минимизации ущерба от инцидентов».
3	Практическое занятие №3 В результате студент докладывает по теме «Угрозы безопасности информационных технологий», «Виды мер и основные принципы обеспечения безопасности информационных технологий», «Правовые основы обеспечения безопасности информационных технологий».
4	Практическое занятие №4 В результате студент докладывает по теме «Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты», Аппаратно-программные средства защиты информации от несанкционированного доступа», «Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа».

№ п/п	Тематика практических занятий/краткое содержание
5	Практическое занятие №5 В результате студент докладывает по теме «Проблемы обеспечения безопасности в компьютерных системах и сетях», «Назначение, возможности, и основные защитные механизмы межсетевых экранов», «Виртуальные частные сети», «Возможности сканеров безопасности».
6	Практическое занятие №6 В результате студент докладывает по теме «Мониторинг событий безопасности», «Стандартны и критерии проведения аудита информационной безопасности», «Методология аудита информационной безопасности», «Организация процесса аудита».
7	Практическое занятие №7 В результате студент докладывает по теме «Основные приборы и оборудование, применяемое для выявления технических каналов утечки информации», «Основы организации и обеспечения работ по технической защите информации», «Технические средства защиты информации и организация работ по защите информации».
8	Практическое занятие №8 В результате студент докладывает по теме «Понятие о компьютерных инцидентах», «Расследование инцидентов в российской федерации и за рубежом», Средства контроля коммуникаций и средств ЭВТ».
9	Практическое занятие №9 В результате студент докладывает по теме «Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях», «Порядок работы с носителями ключевой информации».

4.3. Самостоятельная работа обучающихся.

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

4.4. Примерный перечень тем курсовых работ

Примерные темы курсовой работы: -Особенности обеспечения информационной безопасности микропроцессорных систем управления; -Сертификация средств защиты информации по требованиям ФСБ; -Особенности обеспечения информационной безопасности защищенных помещений; -Особенности утечки информации по ПЭМИН; -Особенности обеспечения информационной безопасности объектов вычислительной техники; -Особенности утечки информации по закрытому каналу связи (Intranet); -Сертификация средств защиты информации по требованиям

ФСТЭК; -Утечки информации по виброакустическому каналу; -Особенности утечки информации по открытому каналу Ethernet; -Особенности обеспечения информационной безопасности на транспортных средствах; -Особенности утечки информации по акустоэлектрическому каналу; -Классификация объектов информатизации по требованиям информационной безопасности; -Особенности обеспечения информационной безопасности диспетчерских систем управления.

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

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга Издательский центр "Академия" , 2012	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)
2	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта В.В. Яковлев, А.А. Корниенко Однотомное издание УМК МПС России , 2002	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
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)

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.
MathCAD 14.0 или другая система моделирования.

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:

Зачет в 10 семестре.
Курсовая работа в 10 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, к.н. кафедры «Управление и защита информации» А.А. Привалов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин