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)

Объекты защиты информации

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 изучения дисциплины «Объекты защиты информации» является обеспечение приобретения специалистами знаний о видах и направлениях защиты информации, сущности и свойств объектов, на которые направлена деятельность, называемая защитой информации. Основной целью изучения учебной дисциплины «Объекты защиты информации» является формирование у обучающегося компетенций для следующих видов деятельности: контрольно-аналитическая; эксплуатационная; специализация №8.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с типами задач профессиональной деятельности): контрольно-аналитическая деятельность: выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты и анализ результатов; проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы; эксплуатационная: установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения; 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-14 - Способен проводить моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации;

ПК-21 - Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой;

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 методы и подходы к моделированию защищенных автоматизированных систем для анализа их уязвимостей.
- Классификацию и характеристику возможных угроз безопасности информации, обрабатываемой в автоматизированных системах.
- Структуру и содержание плана мероприятий по защите информации в объектах информатизации.
- Критерии и методики проведения анализа эффективности систем защиты информации в объектах информатизации.
- Основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.
- Основные принципы разработки нормативных правовых актов, руководящих и методических документов предприятия в области защиты информации.

Уметь:

- На основании проведенного моделирования определять эффективность средств и способов защиты информации.
- Выявлять и классифицировать возможные угрозы безопасности информации, обрабатываемой в автоматизированной системе.
- Разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.
- Применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации.

- Создавать системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

- Разрабатывать нормативные правовые акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности.

Владеть:

- Навыками моделирования защищенных автоматизированных систем и анализа их уязвимостей.

- Методами определения и анализа угроз безопасности информации в автоматизированных системах.

- Навыками разработки документации по планированию мероприятий по защите информации на объектах информатизации.

- Навыками проведения анализа эффективности систем защиты информации и интерпретации его результатов.

- Навыками создания и сопровождения систем обеспечения информационной безопасности на объектах информатизации.

- Навыками разработки нормативной правовой и организационно-распорядительной документации в сфере защиты информации.

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):	80	80
В том числе:		
Занятия лекционного типа	32	32
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 64 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: - Защита информации как деятельность. - Виды защиты информации
2	Основные понятия в области техничской защиты информации. Рассматриваемые вопросы: - Концептуальные основы защиты информации. - Система документов по технической защите информации. - Органы по технической защите информации в РФ. - Лицензирование деятельности в области технической защиты информации.
3	Сертификация средств защиты информации. Рассматриваемые вопросы: - Особенности сертификации средств защиты информации. - Аттестация объекта информатизации по требованиям безопасности информации. - Классификация угроз и объектов защиты.
4	Цели, направления и объекты защиты информации. Рассматриваемые вопросы: - основные цели, направления и объекты защиты информации. - Защита информации от непреднамеренного воздействия
5	Объект информатизации. Рассматриваемые вопросы: - Объект информатизации. - Классификация объектов защиты. - Угрозы несанкционированного доступа к информации. - Основные классы атак в сетях на базе TCP/IP. - Программно-математическое воздействие.
6	Защита информации. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- основные требования и рекомендации по защите информации. - Порядок обеспечения защиты информации в АС.
7	Каналы утечки информации Рассматриваемые вопросы: - основные каналы утчеки информации
8	Классификация канлов утечки информации Рассматриваемые вопросы: - Классификация технических каналов утечки информации. - Информационный сигнал и его характеристики. - Технические каналы утечки акустической информации. - Побочные электромагнитные излучения и наводки.
9	Методы защиты информации от утечки Рассматриваемые вопросы: - Побочные электромагнитные излучения и наводки. - Методы защиты информации от утечки через ПЭМИН.
10	Методы и средства защиты от утечки информации Рассматриваемые вопросы: - основные методы и средства защиты от утечки информации
11	Обнаружение каналов утечки информации Рассматриваемые вопросы: - Средства и методы обнаружения технических каналов утечки информации.
12	Мероприятия по выявлению технических каналов утечки информации. Рассматриваемые вопросы: - основные мероприятия по выявлению технических каналов утечки информации.
13	Оценка защищенности информации от утечки по ТКУИ. Рассматриваемые вопросы: - Оценка защищенности информации от утечки по ТКУИ.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Анализ нормативно-правовой базы технической защиты информации В результате выполнения практического задания студент изучает систему документов по технической защите информации, органы по ТЗИ в РФ, порядок лицензирования и сертификации.
2	Классификация объектов информатизации и угроз безопасности В результате работы студент осваивает классификацию объектов защиты, угроз несанкционированного доступа и основных классов сетевых атак.
3	Выявление вредоносных программ и анализ активности В результате выполнения практического задания студент учится обнаруживать вредоносные программы на компьютере и анализировать подозрительную сетевую активность.
4	Анализ технических каналов утечки информации В результате работы студент изучает классификацию технических каналов утечки информации, информационный сигнал и его характеристики.
5	Методы защиты от утечки информации по техническим каналам В результате работы студент рассматривает основные методы и средства защиты информации от утечки через ПЭМИН и другие технические каналы.

№ п/п	Тематика практических занятий/краткое содержание
6	Средства и методы обнаружения каналов утечки В результате выполнения практического задания студент знакомится с приборами и методиками выявления технических каналов утечки информации.
7	Управление правами пользователей в операционных системах В результате работы студент отрабатывает навыки управления правами пользователей и разграничения доступа к ресурсам (на примере ОС семейства Windows).
8	Анализ и настройка реестра Windows для обеспечения безопасности В результате выполнения практического задания студент учится работать с реестром, выявлять и устранять угрозы, связанные с его настройками.
9	Моделирование технической разведки для объекта информатизации В результате работы студент выполняет моделирование действий технической разведки на основе исходных данных для конкретного объекта информатизации.
10	Оценка защищенности информации от утечки по техническим каналам В результате работы студент осваивает методики оценки защищенности информации от утечки по ТКУИ.
11	Разработка мероприятий по защите информации на объекте В результате работы студент разрабатывает комплекс мероприятий по выявлению и блокированию технических каналов утечки информации.
12	Аттестация объектов информатизации по требованиям безопасности В результате работы студент изучает порядок и особенности аттестации объектов информатизации по требованиям безопасности 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. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Комплексная система защиты информации Буранова М.А., Киреева Н.В. Учебное пособие Самара: ПГУТИ, - 145 с. , 2019	https://reader.lanbook.com/book/223181#2
2	Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) Алешкин А.С., Лесько С.А.,	https://reader.lanbook.com/book/167600#2

	Жуков Д.О. Учебное пособие М.: МИРЭА, — 152 с. , 2020	

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’11, интегрированная среда разработки программного обеспечения для эиуляции сетевого оборудования OmniGraffle;

среда разработки программного обеспечения HTML5 и PHP.

комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ: в области 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:

Зачет 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