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 бакалавриата
по направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Комплексное обеспечение защиты объекта информатизации

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Цели и задачи изучения дисциплины «Комплексное обеспечение защиты объекта информатизации» соотносятся с общими целями ГОС ВПО по специальности/направлению подготовки. Слушатель получает систематизированные теоретические и практические знания в области информационной безопасности. Целью изучения дисциплины является формирование у студентов целостных представлений о всестороннем обеспечении защиты различных объектов информатизации.

Задачами освоения дисциплины являются:

• формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ состояния комплексной информационной безопасности на предприятии;

• изучение основ построения и реализации комплексной системы защиты информации объекта информатизации;

• изучение принципов и общих методов обеспечения информационной безопасности;

• изучение механизмов решения типовых задач программно-аппаратной защиты информации;

• формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ состояния комплексной информационной безопасности на предприятии;

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Эксплуатационная:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологическая:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

- проведение проектных расчетов элементов систем обеспечения информационной

безопасности;

- участие в разработке технологической и эксплуатационной документации;

- проведение предварительного технико-экономического обоснования проектных расчетов

Экспериментально-исследовательская деятельность:

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

- проведение экспериментов по заданной методике, обработка и анализ их результатов;

- проведение вычислительных экспериментов с использованием стандартных программных средств

Организационно-управленческая деятельность:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

- организация работы малых коллективов исполнителей;

- участие в совершенствовании системы управления информационной безопасностью;

- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;

- контроль эффективности реализации политики информационной безопасности объекта защиты.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-4 - способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ;

ПК-7 - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ;

ПК-12 - способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ;

ПК-13 - способностью организовывать работу малого коллектива

исполнителей в профессиональной деятельности.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- современные комплексы мер по обеспечению информационной безопасности$
- основные средства защиты информации, способы защиты информации от НСД$
- основные направления обеспечения информационной безопасности.

Уметь:

- разрабатывать предложения по совершенствованию системы защиты объектов информатизации от НСД$
- организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности;
- выявлять потенциальные каналы утечки информации;
- определять виды информации подверженные атакам потенциального злоумышленника;
- разрабатывать и реализовывать комплексные меры, обеспечивающие эффективность системы защиты информации.

Владеть:

Владеть:

- методологией выбора информационных ресурсов, подлежащий защите;
- разработкой предложения по совершенствованию системы защиты объектов информатизации;
- способностью обоснования критериев эффективности функционирования защищенных автоматизированных систем.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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. №8
Контактная работа при проведении учебных занятий (всего):	52	52
В том числе:		
Занятия лекционного типа	26	26
Занятия семинарского типа	26	26

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 56 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	1. Объекты информатизации и их классификация. 2. Информация как предмет защиты. Содержание: - Сущность и понятие информационной безопасности. -Значение информационной безопасности и ее место в системе национальной безопасности. - Современная доктрина информационной безопасности Российской Федерации. -Понятие и назначение доктрины информационной безопасности. 3. Правовое обеспечение информационной безопасности. Содержание: -Основные законодательные акты, содержащие правовые нормы, направленные на защиту информации. - Правовая защита открытой, общедоступной информации 4. Информация ограниченного доступа Государственная система правовой защиты государственной

№ п/п	Тематика лекционных занятий / краткое содержание
	тайны. Особенности правовой защиты различного вида тайн. 5. Защита и обработка конфиденциальных документов. 6. Технология конфиденциального документооборота. Содержание: -Стадии обработки и защиты конфиденциальных документов входного потока. - Стадии обработки и защиты конфиденциальных документов выходного потока. 7. Идентификация, аутентификация и авторизация. Содержание: -Роль, задачи и факторы аутентификации. - Классификация процессов аутентификации. 8. Угрозы безопасности информации. Содержание: -Угрозы безопасности информации от несанкционированного доступа и возможные последствия от их реализации. - Выбор и содержание мер защиты информации от несанкционированного доступа. -Требования к средствам защиты информации от несанкционированного доступа на объектах информатизации. 9. Электронные замки и аппаратно-программные модули доверенной загрузки. Содержание: -Типовые модели управления доступа субъектов доступа к объектам доступа. - Назначение и основные возможности системы защиты информации от несанкционированного доступа. -Подсистема управления доступом и разграничение доступа к объектам. 10. Инженернотехническая защита информации. Содержание: -Способы и средства добывания информации техническими средствами. -Технические каналы утечки информации. 11. Методы, способы и средства инженернотехнической охраны объекта. Содержание: -Способы и средства защиты информации от наблюдения. -Способы и средства защиты информации от подслушивания. -Основы методического обеспечения инженернотехнической защиты информации. 12. Криптографические методы и средства обеспечения информационной безопасности. Содержание: -Основные задачи современной криптографии. Шифры перестановки, шифры замены, шифры гаммирования. -Блочные и поточные системы шифрования. -Системы шифрования с открытыми ключами. -Электронные цифровые подписи. 13. Сущность и задачи комплексной системы защиты информации (КСЗИ). Содержание: -Принципы организации КСЗИ. -Технология организации КСЗИ.

№ п/п	Тематика лекционных занятий / краткое содержание
	-Разработка модели КСЗИ. - Обеспечение функционирования КСЗИ.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	1. Теория информационной безопасности и методология защиты информации. В результате выполнения работы студент получит практические навыки использования основы правовых знаний в различных сферах деятельности 2. Правовое обеспечение информационной безопасности В результате выполнения работы студент получит практические навыки выделение основных компонентов системы российского права и выделение нормативно правовых актов в сфере информационной безопаности. 3. Организационное обеспечение информационной безопасности В результате выполнения работы студент получит практические навыки принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности 4. Программноаппаратная зашита информации и защита информационных процессов в компьютерных системах. В результате выполнения работы студент получит практические навыки применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения 5. Сущность и задачи комплексной системы защиты информации (КСЗИ). В результате выполнения работы студент получит практические навыки разрабатывать и реализовывать политики управления доступом в компьютерных системах 6. Назначение, структура и содержание управления КСЗИ. В результате выполнения работы студент получит практические навыки организации и этапы разработки комплексной системы защиты информации

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
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. Методологические основы организации комплексной системы защиты информации

2. Система управления информационной безопасностью предприятия.

3. Классификация информации по видам тайны и степеням конфиденциальности

4. Порядок внедрения Перечня сведений, составляющих коммерческой тайны, внесение в него изменений и дополнений

5. Этапы разработки комплексной системы защиты информации

6. Проектирование системы защиты информации для существующей АС

7. Технологическое и организационное построение комплексной системы защиты информации

8. Назначение, структура и содержание управления комплексной системы защиты информации

9. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций

10. Факторы, определяющие необходимость защиты периметра и здания предприятия

11. Особенности помещений как объектов защиты для работы по защите информации

12. Факторы, создающие угрозу информационной безопасности

13. Угрозы безопасности информации

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

№ п/п	Библиографическое описание	Место доступа
1	Защита от вирусов, межсетевые экраны и другие механизмы обеспечения безопасности информационных систем : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех." / В.П. Соловьев, Д.В. Иванов, Н.Н. Пуцко; Ред. В.П.	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/04-35013.pdf.Библиогр.: с. 115 (7 назв.). - Б. ц. - Текст : непосредственный.(дата обращения 04.10.2022)

	Соловьев ; МИИТ. Центр компетентности "Защита и безопасность информации". - М. : МИИТ, 2007. - 115 с. : ил. - (Инновационная образовательная программа - МИИТ).	
2	Методы предотвращения и обнаружения вторжений : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех." / В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев ; МИИТ. Центр компетентности "Защита и безопасность информации". - М. : МИИТ, 2007. - 76 с. : ил. - (Инновационная образовательная программа - МИИТ).	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/04-35222.pdf. - Б. ц. - Текст : непосредственный.
3	Безопасность операционных систем : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех." / В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев ; МИИТ. Центр компетентности "Защита и безопасность информации". - М. : МИИТ, 2007. - 98 с. : ил. - (Инновационная образовательная программа - МИИТ).	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/04-35012.pdf. - Б. ц. -Текст : непосредственный. (дата обращения 04.10.2022)
4	Защищенные беспроводные и мобильные коммуникации : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/04-35015.pdf. - Библиогр.: с. 120 (7 назв.). - Б. ц. - Текст : непосредственный.

	защита инф-ции" напр. "Информатика и выч. тех." / В.П. Соловьев, Д.В. Иванов, Н.Н. Пуцко; Ред. В.П. Соловьев ; МИИТ. Центр компетентности "Защита и безопасность информации". - М. : МИИТ, 2007. - 121 с. : ил. - (Инновационная образовательная программа - МИИТ).	

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

Современные профессиональные базы данных и информационные справочные системы не требуются.

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)

Для проведения практических занятий необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:

• Foxit Reader/Acrobat Reader

• Microsoft Office (Word).

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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 практических работ: компьютеры с предустановленным Microsoft Windows не ниже Windows XP и процессором не ниже Pentium 4.

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

9. Форма промежуточной аттестации:

Курсовой проект в 8 семестре.
Экзамен в 8 семестре.

10. Оценочные материалы.

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

Авторы

Антошкин
Станислав
Владимирович

Лист согласования

Заведующий кафедрой ВССиИБ	Б.В. Желенков
Председатель учебно-методической комиссии	Н.А. Клычева