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 магистратуры
по направлению подготовки
09.04.03 Прикладная информатика,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Системы защиты информационного пространства субъектов экономической деятельности

Направление подготовки: 09.04.03 Прикладная информатика

Направленность (профиль): Информационные технологии управления социально-экономическими системами

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины является формирование у будущих специалистов теоретических знаний и практических навыков в области защиты информационного пространства субъектов экономической деятельности.

Учебные задачи дисциплины определены в соответствии с утвержденными Государственными образовательными стандартами высшего образования и включают следующие задачи:

1. Дать представление о целостной системе знаний в области обеспечения информационной безопасности организации и оценки ее деятельности

2. Изложить базовые правовые нормы, закрепляющие права субъектов экономической деятельности на защиту информации

3. Изложить основные направления развития методологий и технологий проектирования систем защиты информации в корпоративных системах

4. Изучить основы управления инцидентами компьютерной безопасности.

5. Раскрыть понятийно-терминологический аппарат, характеризующий сущность и содержание эффективных методов реализации информационных процессов и построения систем защиты информации

6. Изучить основные методы и технологии создания, сопровождения и эксплуатации информационных систем, обеспечивающих защиту информации

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-5 - Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;

ПК-3 - Способен проектировать архитектуру ИС предприятий и организаций и принимать эффективные проектные решения в условиях неопределенности и риска.

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

Уметь:

-использовать в практической деятельности новейшие методологии и технологии проектирования ИС, с учетом требований компьютерной

безопаснсоти;

- выявлять перечень потенцильных угроз безопасности информации;

-формировать стратегию информатизации прикладных процессов, опираясь на современные методологии компьютерных систем.

Знать:

-современные средства и методы в сфере информационной безопасности;

-основные правовые документы в области информационной безопасности;

-аппаратное обеспечение современных информационных технологий защиты информации;

-принципы и технологии организации информационных потоков в управлении данными как в научной деятельности, так и в сфере образования.

Владеть:

-навыками выбора методов и средств защиты информационного пространства с учетом проектных рисков, анализировать и оптимизировать прикладные и информационные процессы, применять современные методы и инструментальные средства в разработке прикладных информационных процессов.

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. №3
Контактная работа при проведении учебных занятий (всего):	24	24
В том числе:		
Занятия лекционного типа	8	8
Занятия семинарского типа	16	16

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 120 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	Основные термины и определения. Рассматриваемые вопросы: - информация, защищаемая информация и ее свойства - виды тайн, основные субъекты и объекты информационной безопасности.
2	Угрозы, уязвимости и каналы утечки информации Рассматриваемые вопросы: -Угрозы безопасности информации, цели. -Естественные и искусственные угрозы. -Каналы утечки информации. Понятие и примеры НСД к информации в компьютерной системе.
3	Общая характеристика методов и средств защиты информации. Рассматриваемые вопросы: - Классификация методов и средств защиты информации. - Понятие и состав системы защиты информации на предприятии. - Политика информационной безопасности (ИБ) предприятия
4	Защита информационного пространства субъектов экономической деятельности Рассматриваемые вопросы: - Компьютерные правонарушения и преступления (УК РФ ст.272-274) -Риски ИБ -Аудит ИБ -Расследование компьютерных преступлений.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Современные средства и методы защиты информации. В результате практического занятия студент изучает: Шифрование информации: математические основы криптографии
2	Современные средства и методы защиты информации. В результате практического занятия студент изучает: Шифрование информации: модулярный шифр и шифр Цезаря
3	Современные средства и методы защиты информации В результате практического занятия студент изучает: Криптографические методы защиты информации: - Вижинера, - Гамильтона
4	Современные средства и методы защиты информации. В результате практического занятия студент изучает: Криптографические методы защиты информации: - блочные шифры
5	Современные средства и методы защиты информации. В результате практического занятия студент изучает: Криптографические методы защиты информации: - Метод Гронсфельда - Метод «Квадрат Полибия»
6	Современные средства и методы защиты информации. В результате практического занятия студент изучает: Криптографические методы защиты информации: - Эль-Гамаля, - RSA.
7	Современные средства и методы защиты информации. В результате практического занятия студент изучает: -Алгоритмы обмена ключами
8	Современные средства и методы защиты информации. В результате практического занятия студент изучает: -Электронная цифровая подпись

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к лабораторным работам
2	Изучение литературы
3	Работа с лекционным материалом
4	Подготовка к промежуточной аттестации.

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

№ п/п	Библиографическое описание	Место доступа

1	Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с.— ISBN 978-5-9916-9043-0.	Юрайт [сайт]. — URL: https://urait.ru/bcode/491249 (дата обращения: 19.04.2023).— Текст : электронный
2	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с.— ISBN 978-5-534-03600-8.	Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 19.04.2023).— Текст : электронный
3	Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с.— ISBN 978-5-534-14590-8.	Юрайт [сайт]. — URL: https://urait.ru/bcode/497002 (дата обращения: 19.04.2023).— Текст : электронный
4	Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — ISBN 978-5-534-12769-0.	Юрайт [сайт]. — URL: https://urait.ru/bcode/496492 (дата обращения: 19.04.2023).— Текст : электронный

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

Обязательный набор:

Официальный сайт РУТ (МИИТ): https://www.miit.ru/

Научно-техническая библиотека РУТ (МИИТ): http:/library.miit.ru

Образовательная платформа «Юрайт»: https://urait.ru/

Электронно-библиотечная система издательства «Лань»: http://e.lanbook.com/

Федеральная служба государственной статистики: https://rosstat.gov.ru/

Библиотека естественных наук РАН: http://www.benran.ru/

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

Обязательный набор:

1. Windows 8
2. Офисный пакет приложений Microsoft Office

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

Для проведения лекционных занятий необходима аудитория с мультимедиа аппаратурой. Для проведения практических занятий требуется аудитория, оснащенная мультимедиа аппаратурой и ПК с необходимым программным обеспечением, и подключением к сети интернет.

9. Форма промежуточной аттестации:

Экзамен в 3 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 «Системы управления транспортной инфраструктурой» И.М. Губенко

Согласовано:

Заведующий кафедрой ИСЦЭ Л.А. Каргина

Председатель учебно-методической комиссии М.В. Ишханян