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)

Основы информационной безопасности

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины (модуля) «Основы информационной безопасности» являются:

– обучить студентов принципам обеспечения информационной безопасности, подходам к анализу информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем;

– содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Задачи изучения дисциплины:

- изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в компьютерных системах;

- изучение типовых угроз безопасности информации при её обработке в компьютерных системах;

- изучение основных принципов обеспечения информационной безопасности;

- изучение основ построения модели угроз и политики безопасности;

- изучение основных моделей управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

ПК-1 - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах.

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

Знать:

- Основные нормативные правовые акты и доктринальные документы (Доктрина информационной безопасности РФ), определяющие национальные интересы в информационной сфере.

- Основные методы и механизмы защиты информации в ОС (управление доступом, аудит, шифрование дисков), в КС (межсетевое экранирование, VPN, IDS/IPS) и в СУБД (избирательное и мандатное управление доступом, шифрование данных, ролевая модель).

- Современные методы и средства оценки защищенности компьютерных систем, включая стандарты и методики (PCI DSS, методики ФСТЭК, BAS (Breach and Attack Simulation) и др.).

Уметь:

- Анализировать события и явления общественной жизни с точки зрения их информационной составляющей и влияния на безопасность.

- Выбирать и применять адекватные программные и аппаратные средства защиты для конкретных условий эксплуатации системы.

- Проводить сбор и анализ исходных данных, необходимых для расчета показателей защищенности информации.

Владеть:

- Навыками критического анализа информации, получаемой из различных источников (СМИ, соцсети, научная литература), для выявления деструктивных воздействий.

- Навыками администрирования средств защиты информации в составе ОС, КС и СУБД (настройка прав доступа, создание правил МЭ, разграничение доступа к таблицам БД).

- Навыками работы со специализированными инструментальными средствами для анализа защищенности (сканеры уязвимостей, фреймворки для пентеста, анализаторы протоколов).

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	Семестр №4
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 28 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	Национальная безопасность Российской Федерации: понятие, структура и место информационной безопасности Рассматриваемые вопросы: - Понятие, сущность и содержание национальной безопасности. - Основные задачи, объекты и субъекты обеспечения национальной безопасности. - Виды безопасности и виды защищаемой информации. - Место и роль России в глобальном информационном пространстве. - Понятие и роль информационной безопасности в обеспечении национальной безопасности государства. - Национальные интересы России в информационной сфере (интересы личности, общества и государства).
2	Система угроз информационной безопасности Российской Федерации Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Общая характеристика проблем обеспечения информационной безопасности. - Виды угроз: угрозы конституционным правам, угрозы информационному обеспечению госполитики, угрозы развитию отечественной индустрии информации. - Классификация угроз безопасности информационных и телекоммуникационных систем. - Модель действий нарушителя. - Внешние и внутренние источники угроз ИБ РФ. - Классификация источников угроз и уязвимостей.
3	Информационное противоборство и информационная война: основные концепции Рассматриваемые вопросы: - Информационная безопасность и информационное противоборство. - Понятие, цели и проблемы информационных войн. - Субъекты информационного противоборства. - Составные части и методы информационного противоборства.
4	Методология и стратегия ведения информационной войны Рассматриваемые вопросы: - Информационная война как целенаправленное воздействие на информационные системы. - Способы перепрограммирования информационных систем (психологические и технические аспекты). - Проблема начала информационной войны. - Обобщенный алгоритм (типовая стратегия) информационной войны. - Основные аспекты и последствия информационной войны.
5	Организационно-правовые основы защиты информации. Классификация автоматизированных систем Рассматриваемые вопросы: - Документы Гостехкомиссии (ФСТЭК) при Президенте Российской Федерации. - Концепции защиты автоматизированных систем (АС) и средств вычислительной техники (СВТ). - Классификация автоматизированных систем и информационных систем по уровню защищенности. - Требования к информационным системам по обеспечению безопасности информации.
6	Система защиты информации от несанкционированного доступа (НСД) Рассматриваемые вопросы: - Основные направления защиты от НСД и способы НСД. - Принципы защиты информации от НСД. - Структура системы защиты информации от НСД: назначение и функции элементов. - Политика безопасности как основа построения системы защиты.
7	Модели управления доступом Рассматриваемые вопросы: - Правила разграничения доступа. - Дискреционная (DAC) и мандатная (MAC) модели управления доступом. - Ролевая модель управления доступом (RBAC). - Атрибутные модели управления доступом (ABAC).
8	Основы криптографической защиты информации Рассматриваемые вопросы: - Основные понятия криптографии: шифрование, дешифрование, ключ. - Предмет и задачи криптографии. Историческая справка. - Требования к криптографическим системам. - Симметричное и асимметричное шифрование (базовые понятия). - Примеры простейших шифров.
9	Идентификация и аутентификация Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Понятия идентификации, аутентификации и авторизации. - Классификация систем аутентификации (по факторам: знание, владение, неотъемлемые характеристики). - Методы аутентификации: парольная, биометрическая, аппаратная (токены, смарт-карты). - Сертификаты и цифровые подписи как средства подтверждения подлинности.
10	Разграничение и контроль доступа Рассматриваемые вопросы: - Разграничение доступа по виду информации, по способам обработки (чтение, запись, исполнение). - Контекстное управление доступом (по времени, по терминалам). - Разделение привилегий и контроль целостности. - Аудит и мониторинг событий доступа.
11	Сетевые методы защиты. Межсетевые экраны Рассматриваемые вопросы: - Технология межсетевых экранов (МЭ) как защита корпоративных сетей от внешних угроз. - Функции МЭ: фильтрация трафика, трансляция адресов, посредничество. - Политика безопасности и ее реализация на МЭ. - Типы межсетевых экранов (фильтрующие, прокси-серверы, stateful inspection).
12	Защищенные каналы связи. Виртуальные частные сети (VPN) Рассматриваемые вопросы: - Основные понятия и функции виртуальных частных сетей (VPN). - Варианты построения защищенных каналов (узел-узел, удаленный доступ). - Протоколы туннелирования (PPTP, L2TP, IPsec). - Средства обеспечения безопасности VPN: шифрование, аутентификация, проверка целостности.
13	Обнаружение и предотвращение вторжений (IDS/IPS) Рассматриваемые вопросы: - Краткая история развития средств обнаружения атак. - Основные понятия: событие, атака, вторжение, сигнатура, аномалия. - Классификация систем обнаружения вторжений (IDS) и предотвращения вторжений (IPS). - Методы обнаружения: сигнатурный анализ и поведенческий анализ (обнаружение аномалий).
14	Вредоносное программное обеспечение и методы антивирусной защиты Рассматриваемые вопросы: - Вирусы как угроза информационной безопасности. - Классификация вредоносного ПО (вирусы, черви, трояны, программы-вымогатели). - Средства антивирусной защиты: сигнатурный и эвристический анализ. - Комплексные системы защиты конечных точек (EDR).
15	Стандартизация в области информационной безопасности Рассматриваемые вопросы: - Характеристика систем стандартизации в области защиты информации (международные, национальные, отраслевые). - Информационная безопасность распределенных систем. - Европейские критерии безопасности информационных технологий (ITSEC) и их эволюция. - Обзор современных стандартов (Common Criteria/ISO 15408, семейство стандартов ISO 27xxx).
16	Комплексный подход к обеспечению информационной безопасности Рассматриваемые вопросы: - Взаимосвязь правовых, организационных и технических мер защиты. - Политика информационной безопасности организации как документ. - Современные тенденции в области угроз и защиты (кибервойны, атаки на критическую инфраструктуру). - Роль человеческого фактора в обеспечении ИБ.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Виды информации и основные методы ее защиты. Анализ информационной инфраструктуры Российской Федерации. Виды информации и основные методы ее защиты, анализ информационной инфраструктуры государства.
2	Основные понятия и общеметодологические принципы обеспечения информационной безопасности. Основные понятия и общеметодологические принципы информационной безопасности.
3	Классификация видов и анализ источников угроз информационной безопасности Российской Федерации. Виды и источники угроз информационной безопасности Российской Федерации.
4	Изучение видов и форм применения информационно-технологического оружия. Виды и формы применения информационно-технологического оружия.
5	Анализ возможных последствий информационной войны. Последствия информационной войны.
6	Причины, виды и каналы утечки информации. Формальная постановка задачи обеспечения безопасности компьютерных систем. 1 Причины, виды, каналы утечки и искажения информации, формальная постановка и решение задачи обеспечения информационной безопасности компьютерных систем.
7	Исследование моделей организации кибернетической безопасности. Модели организации кибернетической безопасности.
8	Реализация моделей дискреционного и ролевого доступа. Модель избирательного (дискреционного) доступа. Модель ролевого (типизованного) доступа.
9	Изучение модели Лендвера-Маклина (MMS) для анализа защищенности систем. Модель Лендвера-Маклина (MMS).
10	Критерии оценки защищенности компьютерных систем. Выбор методов и средств обеспечения ИБ. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.
11	Изучение программно-аппаратных средств обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.
12	Построение системы разграничения доступа в базе данных на основе ролевой модели. Построение системы разграничения доступа в базе данных на основе ролевой модели.
13	Основные понятия криптографической защиты. Реализация простейшего шифра. Основные понятия криптографической защиты информации. Пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы.
14	Классификация систем аутентификации. Применение электронной подписи для контроля целостности. Классификация систем аутентификации. Электронная подпись и ее применение для контроля целостности программ и данных.

№ п/п	Тематика практических занятий/краткое содержание
15	Технология виртуальных частных сетей (VPN). Варианты построения защищенных каналов. Виртуальные частные сети. Варианты построения виртуальных защищенных каналов.
16	Работа с антивирусными комплексами. Восстановление зараженных файлов и профилактика от «троянских программ». Антивирусные программные комплексы. Восстановление зараженных файлов. Профилактика проникновения «троянских программ».
17	Обобщенная архитектура стандартов обеспечения информационной безопасности организации. Обобщенная архитектура стандартов обеспечения информационной безопасности организации.
18	Изучение документов по оценке защищенности автоматизированных систем, действующих в РФ. Документы по оценке защищенности автоматизированных систем в РФ.

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	Основы информационной безопасности Нестеров С. А. Учебник Издательство "Лань", - 3-е изд., стер. - 324 с. - ISBN 978-5--507-490777-6 , 2024	https://reader.lanbook.com/book/370967
2	Криптографическая защита информации Кунин Н. Т. Практикум Изд. МИРЭА - Российский технологический университет. - 66 с. - ISBN 978-5-7339-2447-2 , 2025	https://reader.lanbook.com/book/493382
3	Защита информации Груздева Л. М. Учебное пособие Изд. Российский университет транспорта, - 144 с. - ISBN 978-5-7876-0326-2 , 2019	https://reader.lanbook.com/book/188703

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 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.

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:

Экзамен в 4 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
«Правовое обеспечение
государственного управления и
экономики» Юридического
института Л.М. Малёшина

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин