

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 директором РУТ (МИИТ)
Покусевым О.Н.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 09.04.03 Прикладная информатика

Направленность (профиль): IT-инженер ВСМ

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2017
Подписал: заместитель руководителя Ефимова Ольга
Владимировна
Дата: 01.06.2025

1. Общие сведения о дисциплине (модуле).

Цели дисциплины:

- сформировать базовые и прикладные знания в области информационной безопасности, актуальных угроз и методов защиты данных;
- обучить основным подходам к обеспечению безопасности информационных систем и формированию политики ИБ.

Задачи дисциплины:

- изучить классификацию угроз, уязвимостей и атак на информационные системы;
- ознакомиться с техническими и организационными методами защиты;
- освоить методы криптографической защиты и аутентификации;
- изучить нормативно-правовые аспекты информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте;

ОПК-6 - Способен исследовать современные проблемы и методы прикладной информатики и развития информационного общества;.

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

Знать:

- основные виды угроз безопасности информации;
- модели обеспечения конфиденциальности, целостности и доступности;
- принципы криптографической защиты;
- российское и международное законодательство в сфере ИБ.

Уметь:

- анализировать риски ИБ в ИС;
- применять методы защиты информации в прикладных задачах;
- настраивать базовые средства защиты: межсетевые экраны, антивирусы, контроль доступа;
- разрабатывать политику безопасности организации.

Владеть:

- навыками оценки уровня защищенности систем;
- методами анализа инцидентов ИБ;
- инструментами обнаружения и предотвращения вторжений.

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 №2
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
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 112 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	Основы информационной безопасности Рассматриваемые вопросы: <ul style="list-style-type: none"> – понятие информации и ее свойства; – основные понятия и цели ИБ; – классификация угроз и уязвимостей; – жизненный цикл инцидента.
2	Политики безопасности и управление доступом Рассматриваемые вопросы: <ul style="list-style-type: none"> – управление правами пользователей; – модели контроля доступа (DAC, MAC, RBAC); – политика безопасности организации; – аудит доступа.
3	Криптографические методы защиты информации Рассматриваемые вопросы: <ul style="list-style-type: none"> – симметричное и асимметричное шифрование; – хеш-функции и электронная подпись; – протоколы TLS, SSH, PGP; – инфраструктура открытых ключей (PKI).
4	Безопасность сетей и передача данных Рассматриваемые вопросы: <ul style="list-style-type: none"> – сетевые угрозы и атаки (MITM, DoS, spoofing); – VPN, NAT, firewall; – IDS/IPS-системы; – защита беспроводных сетей.
5	Безопасность веб-приложений Рассматриваемые вопросы: <ul style="list-style-type: none"> – OWASP Top-10; – уязвимости XSS, SQLi, CSRF; – защита на клиенте и сервере; – тестирование безопасности.
6	Риски и инциденты информационной безопасности Рассматриваемые вопросы: <ul style="list-style-type: none"> – управление рисками ИБ; – выявление и реагирование на инциденты; – план непрерывности и восстановления; – SOC и SIEM-системы.
7	Нормативное регулирование и стандарты Рассматриваемые вопросы: <ul style="list-style-type: none"> – законы РФ (ФЗ-152, ФЗ-187, ФСТЭК, ФСБ); – международные стандарты (ISO/IEC 27001); – регламент GDPR; – ответственность и аудит.
8	Тренды и новые вызовы информационной безопасности Рассматриваемые вопросы: <ul style="list-style-type: none"> – ИБ в облачных средах; – безопасность IoT и мобильных устройств; – искусственный интеллект в ИБ; – киберпреступность и хакерские группировки.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Анализ угроз и уязвимостей информационных систем В результате выполнения практической работы студенты выявляют основные типы угроз в заданной ИС.
2	Разработка политики информационной безопасности В результате выполнения практической работы студенты составляют документ политики ИБ для организации.
3	Шифрование и хеширование данных В результате выполнения практической работы студенты реализуют шифрование и хеширование с использованием OpenSSL и Python.
4	Настройка сетевого экрана и VPN В результате выполнения практической работы студенты конфигурируют iptables и создают защищенное соединение VPN.
5	Анализ уязвимостей веб-приложений В результате выполнения практической работы студенты проводят аудит безопасности веб-приложения с помощью Burp Suite.
6	Реагирование на инцидент ИБ В результате выполнения практической работы студенты анализируют лог-файлы и формируют отчет по инциденту.
7	Разбор стандартов ISO/IEC 27001 и Ф3-152 В результате выполнения практической работы студенты сопоставляют нормативные требования с политикой безопасности.
8	Обнаружение атак с использованием SIEM В результате выполнения практической работы студенты анализируют события из демо-данных SIEM-системы.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям
2	Работа с лекционным материалом
3	Самостоятельное изучение рекомендуемой литературы
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н.	https://e.lanbook.com/book/460715

	Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4.	
2	Баланов, А. Н. Создание цифровых экосистем : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 480 с. — ISBN 978-5-507-49668-6.	https://e.lanbook.com/book/428036
3	Баланов, А. Н. Биометрия. Разработка и внедрение систем идентификации : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 228 с. — ISBN 978-5-507-49167-4.	https://e.lanbook.com/book/405494

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/>);

Официальный сайт Минтранса России (<https://mintrans.gov.ru/>);

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

Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru/);

Образовательная платформа «Открытое образование» (<https://openedu.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/>);

Электронно-библиотечная система «Академия» (<http://academia-moscow.ru/>);

Электронно-библиотечная система «BOOK.ru» (<http://www.book.ru/>);

Электронно-библиотечная система «ZNANIUM.COM» (<http://www.znanium.com/>).

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

Visual studio Code

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 во 2 семестре.

10. Оценочные материалы.

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

Авторы:

менеджер

А.А. Кочурков

Согласовано:

Заместитель руководителя

О.В. Ефимова

Председатель учебно-методической
комиссии

Д.В. Паринов