МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
специализированного высшего образования
по направлению подготовки
25.04.03 Аэронавигация,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 25.04.03 Аэронавигация

Направленность (профиль): Интеллектуальные системы обработки информации и управления на воздушном транспорте

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью дисциплины «Основы информационной безопасности» является формирование компетенций о целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Основными задачами дисциплины являются:

• Ознакомление с методами и средствами технической защиты информации;

• Ознакомление с технологическими решениями для обеспечения информационной безопасности в различных сферах;

• Изучение методов организационно-правового обеспечения деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;

• Приобретение навыков установки, настройки, эксплуатации и поддержания в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-1 - Способен управлять работами по созданию (модификации) и сопровождению интеллектуальных информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы на воздушном транспорте.

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

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;

- место информационной безопасности в системе национальной безопасности страны;

- виды, источники и носители защищаемой информации;

- источники угроз безопасности информации и меры по их предотвращению;

- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

- современные средства и способы обеспечения информационной безопасности;

- основные методики анализа угроз и рисков информационной безопасности.

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;

- Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа;

- Настраивать параметры и сегментировать элементы администрируемой сети;

- классифицировать основные угрозы безопасности информации.

Владеть:

- профессиональной терминологией;

-планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа;

- навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и объектов информатизации;

- методами защиты информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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 №3
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

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 132 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 в информационную безопасность Содержание учебного материала: - Понятие информации и информационной безопасности. - Информация, сообщения, информационные процессы как объекты информационной безопасности. - Обзор защищаемых объектов и систем.
2	Основные понятия,термины и определения теории информационной безопасности Содержание учебного материала: - История становления теории информационной безопасности. - Предметная область теории информационной безопасности. - Систематизация понятий в области защиты информации. - Основные принципы построения систем защиты. - Концепция комплексной защиты информации. - Задачи защиты информации. - Средства реализации комплексной защиты информации.
3	Информация как объект защиты. Информационные ресурсы и их защита Содержание учебного материала: - Понятие об информации как объекте защиты. - Уровни представления информации. Основные свойства защищаемой информации. - Виды и формы представления информации. - Информационные ресурсы.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Структура и шкала ценности информации. - Классификация информационных ресурсов. - Правовой режим информационных ресурсов.
4	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности Содержание учебного материала: - Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. - Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
5	Угрозы информационной безопасности Содержание учебного материала: - Анализ уязвимостей системы. - Классификация угроз информационной безопасности. - Основные направления и методы реализации угроз. - Неформальная модель нарушителя. - Оценка уязвимости системы.
6	Построение систем защиты от угрозы нарушения конфиденциальности Содержание учебного материала: - Определение и основные способы несанкционированного доступа. - Методы защиты от НСД. - Организационные методы защиты от НСД. - Инженерно-технические методы защиты от НСД. - Построение систем защиты от угрозы утечки по техническим каналам.
7	Методы контроля доступа к информации Содержание учебного материала: - Идентификация и аутентификация. - Основные направления и цели использования криптографических методов. - Защита от угрозы нарушения конфиденциальности на уровне содержания информации. - Защита целостности информации при хранении. - Защита целостности информации при обработке. Защита целостности информации при транспортировке. - Защита от угрозы нарушения целостности информации на уровне содержания. - Построение систем защиты от угрозы отказа доступа к информации. - Защита семантического анализа и актуальности информации.
8	Обзор международных стандартов информационной безопасности Содержание учебного материала: - Роль стандартов информационной безопасности. - Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. - Европейские критерии безопасности информационных технологий (ITSEC). - Федеральные критерии безопасности информационных технологий США. - Единые критерии безопасности информационных технологий. - Группа международных стандартов 270000.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Симметричное шифрование: AES в различных режимах (ECB, CBC, GCM) В результате выполнения лабораторной работы студент получит навыки реализа-ции шифрования и дешифрования данных с использованием AES, анализа уязви-мостей режима ECB (например, при работе с изображениями), выбора режимов CBC и GCM для обеспечения конфиденциальности и целостности.
2	Асимметричная криптография: генерация ключей RSA и обмен зашифрованными сообщениями В результате выполнения лабораторной работы студент получит навыки генера-ции публичных и приватных ключей, шифрования сообщения публичным клю-чом получателя, дешифрования приватным ключом, а также понимания вычисли-тельной сложности атак на короткие ключи.
3	Электронная подпись (RSA-PSS / ECDSA) и проверка подлинности данных В результате выполнения лабораторной работы студент получит навыки создания цифровой подписи для файла, экспорта подписи в отдельный файл, проверки подписи с использованием публичного ключа, а также обнаружения факта моди-фикации данных после подписания.
4	Криптографическое хэширование (SHA-256, MD5) и его применение для кон-троля целостности В результате выполнения лабораторной работы студент получит навыки вычис-ления хэшей файлов, сравнения хэшей для обнаружения изменений (в т.ч. бито-вых), понимания коллизий на примере MD5 и выбора стойких алгоритмов для хранения паролей.
5	Атака «человек посередине» (MITM) на протокол обмена ключами Диффи — Хеллмана В результате выполнения лабораторной работы студент получит навыки перехва-та и подмены публичных ключей в незащищенном канале, расшифровки трафика без ведома сторон, а также практического понимания необходимости аутентифи-кации ключей (PKI).
6	Анализ сетевого трафика с Wireshark: перехват паролей по протоколам HTTP, FTP, Telnet В результате выполнения лабораторной работы студент получит навыки захвата пакетов в локальной сети, фильтрации трафика по протоколам, восстановления передаваемых логинов и паролей из plain-text протоколов, а также обнаружения подозрительных соединений.
7	ARP-spoofing: перехват трафика в локальной сети с помощью BetterCAP / Ettercap В результате выполнения лабораторной работы студент получит навыки отравле-ния ARP-таблиц, организации MITM между жертвой и шлюзом, перехвата HTTP-сессий, а также настройки статических ARP-записей как метода защиты.
8	Сканирование портов и ОС с помощью Nmap (TCP SYN, FIN, XMAS) и обход простых файрволов

№ п/п	Тематика практических занятий/краткое содержание
	В результате выполнения лабораторной работы студент получит навыки прове-дения скрытого сканирования, определения открытых портов и сервисов, иден-тификации ОС по отпечаткам стека TCP/IP, а также анализа защищенности сете-вых периметров.
9	Обнаружение вторжений (IDS): настройка Snort для сигнатурного анализа трафика В результате выполнения лабораторной работы студент получит навыки написания собственных сигнатур (правил) Snort, перехвата подозрительных пакетов (например, с признаками SQL-инъекции или сканирования портов), генерации оповещений и логирования атак.
10	Защита от DDoS: настройка rate limiting и синхронных кук (SYN cookies) на Linux (iptables) В результате выполнения лабораторной работы студент получит навыки ограничения числа соединений с одного IP, защиты от SYN-flood с включением SYN cookies, эмуляции атаки с помощью hping3, а также анализа загрузки сервера под атакой.
11	Сегментация сети и межсетевые экраны (pfSense): правила пропуска трафика между VLAN В результате выполнения лабораторной работы студент получит навыки создания VLAN, настройки правил allow/deny для разных зон (DMZ, LAN, Guest), органи-зации NAT, а также проверки изоляции сегментов с помощью сканирования.
12	SQL-инъекции (SQLi) вручную и через sqlmap: извлечение данных из базы В результате выполнения лабораторной работы студент получит навыки обнаружения уязвимых параметров, использования UNION и слепых инъекций (boolean/time-based) для обхода авторизации, дампа таблиц, а также применения параметризованных запросов для защиты.
13	Межсайтовый скриптинг (XSS): кража сессий и подмена контента (stored / reflected / DOM) В результате выполнения лабораторной работы студент получит навыки внедрения JavaScript-кода в комментарии или параметры URL, перехвата cookie жертвы с отправкой на внешний сервер, создания поддельных форм ввода, а также настройки Content-Security-Policy (CSP).
14	CSRF (межсайтовая подделка запроса): атака на смену пароля без ведома пользователя В результате выполнения лабораторной работы студент получит навыки создания вредоносной HTML-страницы с автоматической отправкой POST-запроса, перехвата валидной сессии, а также внедрения anti-CSRF токенов и проверки Referer-заголовков как метода защиты.
15	Небезопасные десериализация в Java/Python: удаленное выполнение кода (RCE) В результате выполнения лабораторной работы студент получит навыки создания вредоносного сериализованного объекта, эксплуатации гаджет-цепочки (например, ysoserial), получения reverse shell, а также санитизации и белого списка клас-сов при десериализации.

№ п/п	Тематика практических занятий/краткое содержание
16	XXE (XML External Entity): чтение локальных файлов и SSRF через парсер XML В результате выполнения лабораторной работы студент получит навыки внедрения внешней сущности для чтения /etc/passwd, организации запроса к внутренним серверам (SSRF), проведения DoS через «billion laughs», а также отключения об-работки external entities в парсере.

4.3. Самостоятельная работа обучающихся.

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

4.4. Примерный перечень тем курсовых работ

1. Формы психологической защиты человека от информационной перегрузки.

2. Социально вредная информация в СМИ.

3. Вредная и опасная информация в Интернет

4. Формы обмана и мошенничества в Интернет.

5. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.

6. Модель информационной защиты каналов связи.

7. Стратегия обмана и ее использование в сфере информационной защиты.

8. Вопросы информационной безопасности в политике и дипломатии.

9. Организационно-распорядительные меры информационной защи-ты.

10. Традиционные направления информационной защиты и пути их интеграции.

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

№ п/п	Библиографическое описание	Место доступа
1	Кодирование и защита информации в документооборо-те: метод. указ. к практ. и лаб. раб. для студ. спец. Прикладная информатика (в экономике) по дисц. Информационная безопасность / В.И. Морозова, К.Э. Врублевский; МИИТ. Каф. Экономическая информатика. - М.: МИИТ, 2010. - 56 с.	URL: 03_19830.pdf (miit.ru). (дата обращения 03.03.2024) Текст : непосредственный.004.056.57 М 80
2	Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф. Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с.	URL: 04-46051.pdf (miit.ru). (дата обращения 03.03.2024) Текст : непосредственный.004 К 72
3	Криптографическая защита компьютерной информации: метод. указ. к лаб. раб. по дисц. Теоретические основы компьютерной безопасности для студ., обуч. по напр. Информационная безопасность / Я. М. Голдовский, Б. В. Желенков, И. Е. Сафонова; МИИТ. Каф. Вычислительные системы и сети. - М.: МГУПС(МИИТ), 2013. - 36 с.	URL: 03-42764.pdf (miit.ru). (дата обращения 03.05.2026) Текст : непосредственный.004 Г60
4	Информационная безопасность персональных компьютеров: учеб. пособие для студ. спец. САПР и строительных спец. по курсу Методы и средства защиты компьютерной информации. Ч.2 / В.Ю. Смирнов, О.В. Смирнова; МИИТ. Каф. САПР транспортных конструкций и сооружений.М.: МИИТ, 2010. - 88 с.	URL: 10-2256.pdf (miit.ru). (дата обращения 03.05.2026) Текст : непосредственный.681.3.066 С 50
5	Разработка мер защиты информационных ресурсов в корпоративной сети с выходом в интернет: учебно-метод. пособие по курс. работе для специалистов напр. Компьютерная безопасность / В. М. Алексеев; МИИТ. Каф. Управление и защита информации. - М.: РУТ(МИИТ), 2017. - 9 с.	URL: DC-435.pdf (miit.ru). (да-та обращения 03.05.2026) Текст : непосредственный.004 А-47

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

- Научная электронная библиотека (http://elibrary.ru)
- Материалы по информационным технологиям (www.citforum.ru)
- Официальный сайт РУТ (МИИТ) http://miit.ru
- Научно-техническая библиотека РУТ (МИИТ): http://library.miit.ru

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

- Интернет-браузер (Yandex и др.)
- Microsoft Windows.
- Microsoft Office

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, лабораторных работ, курсового проектирования (выполнения курсовых работ):

- компьютер преподавателя, мультимедийное оборудование, рабочие станции студентов, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет 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
«Вычислительные системы и
квантовые коммуникации» Я.М. Голдовский

Согласовано:

Заместитель директора академии Д.Е. Гончаров

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии В.В. Безряков