

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ))



Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы управления информационной безопасностью

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей
(в сфере связи, информационных и
коммуникационных технологий)

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 ФГАОУ ВО РУТ
(МИИТ)

ID подписи: 4196

Подписал: заведующий кафедрой Желенков Борис
Владимирович

Дата: 25.09.2026

1. Общие сведения о дисциплине (модуле).

Целью изучения дисциплины «Основы управления информационной безопасностью» является формирование у обучающихся компетенций в области управления информационной безопасностью компьютерных систем. Слушатели получают систематизированные теоретические знания и практические навыки, необходимые для формализации задач управления безопасностью и анализа рисков функционирования компьютерных систем, а также для разработки технических заданий, проектирования и исследования подсистем информационной безопасности с учетом требований стандартов и технико-экономических обоснований.

Для достижения цели студенты изучают принципы построения и жизненный цикл системы управления информационной безопасностью, модели угроз и нарушителя, формальные модели политик безопасности, методы анализа и оценки рисков, а также стандарты и нормативные документы в области управления информационной безопасностью. Они получают навыки определения защищаемых ресурсов и требований к их защите, разработки технических заданий, выбора и обоснования проектных решений и оценки эффективности функционирования подсистем информационной безопасности.

Задачами освоения дисциплины являются:

- ознакомление с основными принципами построения информационной безопасности объекта защиты;
- формирование навыков по определению информационных ресурсов, подлежащих защите;
- изучение и определение возможных источников и видов угроз безопасности информации;
- получение навыков по реализации СУИБ на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.
- изучение методов управления СУИБ на предприятии
- получение знаний об основных методах контроля обеспечения информационной безопасности в организации
- формирование навыков построения политики информационной безопасности организации

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-5 - Способность формализовывать задачи управления безопасностью и анализировать риски функционирования компьютерных систем;

ПК-8 - Способность разрабатывать технические задания, проектировать и исследовать подсистемы информационной безопасности автоматизированных систем с учетом требований стандартов и технико-экономических обоснований.

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

Знать:

- основные понятия, принципы и модели управления информационной безопасностью компьютерных систем, структуру и жизненный цикл системы управления информационной безопасностью;
- основные виды угроз и рисков функционирования компьютерных систем, методы их выявления, анализа и оценки;
- методы формализации задач управления безопасностью компьютерных систем (модели угроз и нарушителя, модели рисков, формальные модели политик безопасности);
- порядок разработки технических заданий на создание подсистем информационной безопасности, стадии создания автоматизированных систем в защищённом исполнении;
- нормативные и методические документы, регламентирующие проектирование и обеспечение информационной безопасности компьютерных систем (ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27005, ГОСТ 34.602, документы ФСТЭК России).

Уметь:

- формализовывать задачи управления безопасностью компьютерных систем с учетом выявленных угроз и рисков;
- выявлять, анализировать и оценивать риски функционирования компьютерных систем, выбирать способы их обработки;
- определять требования к подсистемам информационной безопасности и разрабатывать технические задания на их создание и модернизацию;
- проектировать подсистемы информационной безопасности с учетом требований стандартов и обосновывать проектные решения, в том числе технико-экономически;
- проводить исследование и оценку эффективности функционирования подсистем информационной безопасности.

Владеть:

- методами формализации задач управления безопасностью компьютерных систем;
- качественными и количественными методами выявления, анализа и оценки рисков информационной безопасности;
- навыками разработки технических заданий на подсистемы информационной безопасности в соответствии с требованиями стандартов;
- методами проектирования подсистем информационной безопасности и технико-экономического обоснования проектных решений;
- методами исследования и оценки эффективности подсистем информационной безопасности.

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 №7
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
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 80 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 управление информационной безопасностью Краткое содержание: Введение в основы управления информационной безопасностью, обзор основных понятий и принципов, роль информационной безопасности в современных организациях.
2	Законодательные и нормативные основы информационной безопасности Краткое содержание: Обзор законодательных и нормативных актов, регулирующих область информационной безопасности, анализ требований и стандартов.
3	Угрозы информационной безопасности Краткое содержание: Изучение различных типов угроз информационной безопасности, анализ методов их классификации и оценки рисков.
4	Анализ и управление рисками информационной безопасности Краткое содержание: Основы анализа и оценки рисков информационной безопасности, методы управления рисками, выбор и применение контрмер.
5	Планирование и организация информационной безопасности Краткое содержание: Процесс планирования и организации информационной безопасности, разработка политики и стратегии безопасности.
6	Управление доступом и идентификацией Краткое содержание: Основы управления доступом к информационным ресурсам, методы аутентификации и авторизации, управление идентификацией пользователей
7	Защита информационных систем Краткое содержание: Обзор методов и средств защиты информационных систем, принципы построения защищенных архитектур
8	Управление инцидентами информационной безопасности Краткое содержание: Организация процесса управления инцидентами информационной безопасности, реагирование на инциденты, восстановление после инцидентов.
9	Правовые и этические аспекты информационной безопасности Краткое содержание: Рассмотрение правовых и этических вопросов в области информационной безопасности, требования к этическому поведению специалистов.
10	Обучение и осведомленность пользователей Краткое содержание: Разработка и проведение программ обучения и осведомленности пользователей в области информационной безопасности.
11	Аудит информационной безопасности Краткое содержание: Роль и значение аудита в области информационной безопасности, методы и процедуры проведения аудита.
12	Мониторинг и анализ безопасности информационных систем Краткое содержание: Основы мониторинга и анализа безопасности информационных систем, выбор и применение инструментов мониторинга.

№ п/п	Тематика лекционных занятий / краткое содержание
13	Управление уязвимостями информационной безопасности Краткое содержание: Идентификация и управление уязвимостями информационных систем, методы и средства обнаружения и устранения уязвимостей.
14	Бизнес-планирование информационной безопасности Краткое содержание: Разработка бизнес-планов в области информационной безопасности, анализ эффективности инвестиций.
15	Управление изменениями в информационной безопасности Краткое содержание: Организация процесса управления изменениями в области информационной безопасности, анализ рисков при внедрении изменений.
16	Контроль и улучшение процессов информационной безопасности Краткое содержание: Оценка и улучшение эффективности процессов информационной безопасности, выбор и применение методов контроля и анализа.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Тема 1-2: Анализ угроз информационной безопасности Краткое содержание: Студенты изучают основные виды угроз информационной безопасности, такие как внешние и внутренние атаки, вредоносное программное обеспечение, социальная инженерия и утечка данных. Проводится анализ возможных источников угроз, уязвимостей информационных систем и их потенциального воздействия на организацию. В результате работы студенты формируют навыки выявления, анализа и оценки угроз информационной безопасности.
2	Тема 3-4: Разработка политики информационной безопасности Краткое содержание: Студенты разрабатывают политику информационной безопасности для организации, определяют основные принципы и правила, которые должны соблюдаться сотрудниками. В результате работы студенты получают навыки разработки политики информационной безопасности.
3	Тема 5-6: Управление доступом и идентификацией Краткое содержание: Студенты проводят анализ системы управления доступом в организации, определяют требования к аутентификации и авторизации пользователей, разрабатывают рекомендации по улучшению системы. В результате работы студенты получают навыки управления доступом и идентификацией.
4	Тема 7 : Защита информационных систем Краткое содержание: Студенты анализируют защиту информационных систем организации, определяют уязвимые места и разрабатывают план мер по усилению защиты. В результате работы студенты получают навыки анализа и улучшения защиты информационных систем.
5	Тема 8: Управление инцидентами информационной безопасности Краткое содержание: Студенты проводят симуляцию инцидента информационной безопасности, разрабатывают план реагирования на инцидент и восстановления после него. В результате работы студенты получают навыки управления инцидентами информационной безопасности.

№ п/п	Тематика практических занятий/краткое содержание
6	Тема 9: Обучение и осведомленность пользователей Краткое содержание: Студенты разрабатывают программу обучения пользователей в области информационной безопасности, создают обучающие материалы и проводят тренинги. В результате работы студенты получают навыки разработки и проведения программ обучения пользователей.
7	Тема 10: Аудит информационной безопасности Краткое содержание: Студенты проводят аудит информационной безопасности в организации, анализируют соответствие системы безопасности требованиям и стандартам, разрабатывают рекомендации по улучшению. В результате работы студенты получают навыки проведения аудита информационной безопасности.
8	Тема 11: Мониторинг и анализ безопасности информационных систем Краткое содержание: Студенты проводят мониторинг и анализ безопасности информационных систем организации, определяют потенциальные угрозы и разрабатывают план мер по их предотвращению.
9	Тема 13: Управление рисками информационной безопасности Краткое содержание: Студенты изучают основные подходы к оценке и управлению рисками информационной безопасности, проводят практическую оценку рисков для условной организации. Результат: Навыки идентификации, оценки и минимизации рисков информационной безопасности.
10	Тема 14: Защита персональных данных Краткое содержание: Студенты изучают основные принципы и методы защиты персональных данных, разрабатывают модель обработки и защиты данных в организации. Результат: Навыки обеспечения соответствия требованиям по защите персональных данных.
11	Тема 15-16: Итоговая проектная работа и защита Краткое содержание: Студенты разрабатывают и защищают индивидуальные или групповые проекты по выбранной теме, демонстрируя полученные знания и навыки. Результат: Закрепление теоретических знаний через практическую деятельность.

4.3. Самостоятельная работа обучающихся.

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

4.4. Примерный перечень тем курсовых работ

1. Цель и этапы анализа объектов защиты.
2. Идентификация и классификация объектов защиты.
3. Подходы к разграничению доступа в рамках организации. Структура документов, регламентирующих разграничение доступа.

4. Угрозы, источником которых является персонал организации.
5. Обязанности сотрудников Службы безопасности
6. Предоставление сотруднику доступа к конфиденциальной информации
7. Основные положения инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации.
8. Основные положения регламента контроля использования технических средств обработки и передачи информации.
9. Основные положения инструкции по организации парольной защиты.
10. Основные положения документов, регламентирующих использование средств аутентификации и носителей ключевой информации.
11. Основные положения инструкции по организации антивирусной защиты.
12. Основные положения инструкции по работе с электронной почтой.
13. Основные положения плана обеспечения непрерывной работы и восстановления работоспособности

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

№ п/п	Библиографическое описание	Место доступа
1	Позубенкова Э.И. Управление организацией: учебное пособие. Пензенский государственный аграрный университет, 2020.-169с	https://e.lanbook.com/book/170979 (дата обращения: 15.03.2025).- Текст электронный.
2	Троицкая Н.Н. Управление организацией: учебное пособие. Российский университет транспорта, 2019.-83с	https://e.lanbook.com/book/175779 (дата обращения: 15.03.2025).- Текст электронный.
3	Мандыч И. А., Быкова А. В. Управление стратегией организации: учебное пособие. МИРЭА - Российский технологический университет, 2021.-64с	https://e.lanbook.com/book/171536 (дата обращения: 15.03.2025).- Текст электронный.
4	Окладчик С.А. Управление организацией (предприятием): учебное пособие. Иркутский государственный аграрный университет имени А.А. Ежевского, 2020.-112с	https://e.lanbook.com/book/183554 (дата обращения: 15.03.2025).- Текст электронный.

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/>
- Образовательная платформа «Юрайт» <https://urait.ru/>
- ЭБС "Лань" <https://e.lanbook.com/book/>

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

- ОС Windows
- Microsoft Office
- Foxit Reader/Acrobat Reader
- Интернет-браузер (Yandex и др.)

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий):

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

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Курсовая работа в 7 семестре.

Экзамен в 7 семестре.

10. Оценочные материалы.

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

Авторы:

доцент кафедры «Вычислительные
системы и квантовые
коммуникации»

С.В. Антошкин

Согласовано:

Заведующий кафедрой ВСиКК

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Андриянова