

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)

Аудит информационной безопасности

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 «Аудит информационной безопасности» является формирование у обучающихся компетенций в области аудита, анализа и контроля состояния безопасности компьютерных систем. Слушатели получают систематизированные теоретические знания и практические навыки, необходимые для анализа и обеспечения безопасности компьютерных систем, инструментального мониторинга и анализа их защищенности с выявлением уязвимостей и оценкой уровня защищенности, а также для применения аналитических и правовых подходов при расследовании компьютерных инцидентов.

Для достижения цели студенты изучают нормативную правовую базу и стандарты в области аудита и расследования инцидентов, виды, формы и этапы проведения аудита, методы и инструментальные средства анализа защищенности и тестирования на проникновение, а также методы сбора, фиксации и анализа цифровых свидетельств. Они получают навыки планирования и проведения аудиторских проверок, выявления уязвимостей и несоответствий, расследования компьютерных инцидентов, документирования результатов и формирования рекомендаций по повышению уровня защищенности.

Задачами освоения дисциплины являются:

- усвоение знаний по нормативно-правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;
- ознакомление с целями и задачами проведения аудита информационной безопасности объекта защиты;
- ознакомление с основными угрозами информационной безопасности, правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности;
- изучение видов и форм проведения аудита;
- изучение стандартов ИБ;
- получение навыков по использованию методов проведения аудита ИБ;
- получение навыков по выявлению уязвимостей и формированию рекомендаций по совершенствованию системы ИБ.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-2 - Способность проводить анализ и обеспечение безопасности компьютерных систем;

ПК-4 - Способность применять аналитические и правовые подходы в расследовании компьютерных инцидентов;

ПК-10 - Способность осуществлять инструментальный мониторинг и анализ состояния безопасности компьютерных систем и сетей, выявлять уязвимости и оценивать уровень защищенности.

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

Знать:

- основные понятия, цели, задачи, виды и принципы проведения аудита информационной безопасности, нормативные правовые акты и стандарты в области аудита (ГОСТ Р ИСО 19011, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 57580, документы ФСТЭК России);
- методы анализа и обеспечения безопасности компьютерных систем: операционных систем, сетей, СУБД и приложений;
- методы и средства инструментального анализа защищённости, тестирования на проникновение, выявления уязвимостей и оценки уровня защищённости;
- порядок реагирования на компьютерные инциденты, методы сбора, фиксации и анализа цифровых свидетельств;
- правовые основы расследования компьютерных инцидентов и ответственности за преступления и правонарушения в сфере компьютерной информации.

Уметь:

- планировать и проводить аудит информационной безопасности, выявлять несоответствия установленным требованиям;
- анализировать защищённость компьютерных систем и разрабатывать меры по обеспечению их безопасности;
- применять инструментальные средства анализа защищённости и тестирования на проникновение, оценивать уровень защищённости;
- собирать, сохранять и анализировать цифровые свидетельства при расследовании компьютерных инцидентов с соблюдением правовых требований;
- формировать отчёты по результатам аудита и расследования, рекомендации по устранению выявленных нарушений.

Владеть:

- методами сбора и анализа аудиторских свидетельств;
- методами анализа защищённости и обеспечения безопасности компьютерных систем;
- навыками инструментального анализа защищённости и приоритизации уязвимостей;
- методами расследования компьютерных инцидентов и анализа цифровых свидетельств;
- навыками документирования результатов аудита и расследования, подготовки отчётов и рекомендаций.

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 №9
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 аудит информационной безопасности - Определение понятия аудит информационной безопасности - Роль и задачи аудитора информационной безопасности - Значение аудита для обеспечения безопасности информации.
2	Нормативная база аудита информационной безопасности - Обзор основных нормативных документов в области информационной безопасности - Разъяснение требований и рекомендаций по аудиту информационной безопасности.
3	Методы и инструменты аудита информационной безопасности - Основные методы проведения аудита информационной безопасности - Использование специализированных инструментов для проведения аудита.
4	Планирование аудита информационной безопасности - Определение целей и задач аудита информационной безопасности - Разработка плана аудита и его основные этапы.
5	Анализ угроз и уязвимостей информационной безопасности - Идентификация угроз и уязвимостей в информационной системе
6	Анализ угроз и уязвимостей информационной безопасности. Оценка рисков. - Оценка рисков и определение приоритетов для проведения аудита
7	Оценка соответствия политике информационной безопасности - Проверка соответствия политике и процедурам информационной безопасности - Анализ эффективности мер по обеспечению безопасности информации.
8	Аудит физической безопасности информационных ресурсов - Проверка физической защищенности серверных комнат, ЦОД и других объектов - Оценка контроля доступа и мер по предотвращению несанкционированного доступа.
9	Аудит логической безопасности информационных систем - Проверка уровня защиты операционных систем, сетей и баз данных - Оценка правильности настройки системы контроля доступа и аутентификации.
10	Аудит защиты информации от внешних атак - Проверка наличия и эффективности систем защиты от внешних атак - Оценка уровня обнаружения и предотвращения киберугроз.
11	Аудит защиты информации от внутренних угроз - Проверка мер по предотвращению утечки информации внутри организации - Оценка эффективности систем мониторинга и обнаружения нарушений.
12	Аудит безопасности приложений и программного обеспечения - Проверка уровня защиты приложений от взлома и эксплуатации уязвимостей - Оценка процессов разработки и тестирования безопасности приложений.
13	Аудит управления инцидентами информационной безопасности - Проверка готовности и эффективности процессов реагирования на инциденты - Оценка процедур регистрации, анализа и устранения инцидентов.
14	Аудит обучения и осведомленности сотрудников в области информационной безопасности

№ п/п	Тематика лекционных занятий / краткое содержание
	- Проверка эффективности программ обучения и осведомленности сотрудников. - Оценка степени соблюдения правил и политик безопасности.
15	Аудит документирования и архивирования информации - Проверка процессов документирования и архивирования информации - Оценка соответствия требованиям законодательства и политик безопасности.
16	Аудит управления доступом к информационным ресурсам - Проверка процессов управления доступом и привилегиями пользователей - Оценка эффективности механизмов идентификации и аутентификации.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Определение целей и задач аудита информационной безопасности - Обсуждение роли и значимости аудита информационной безопасности - Определение целей и задач аудита для конкретной организации В результате выполнения работы студент получает практические навыки по определению целей и задач аудита информационной безопасности, что позволит студентам лучше понять роль и значимость аудита в организации.
2	Разработка плана аудита информационной безопасности - Определение этапов и последовательности проведения аудита - Разработка плана аудита с учетом специфики организации В результате выполнения работы студент получает практические навыки разработки плана аудита информационной безопасности, что поможет студентам научиться структурировать и организовывать процесс аудита.
3	Идентификация угроз и уязвимостей информационной системы - Анализ существующих угроз и уязвимостей в информационной системе - Оценка рисков и приоритизация для проведения аудита В результате выполнения работы студент получает практические навыки идентификации угроз и уязвимостей информационной системы, что позволит студентам научиться анализировать существующие угрозы и оценивать риски.
4	Проверка соответствия политике информационной безопасности - Анализ политик и процедур информационной безопасности - Оценка соответствия политике и эффективности мер по обеспечению безопасности информации В результате выполнения работы студент получает практические навыки проверки соответствия политике информационной безопасности, что поможет студентам оценить эффективность мер по обеспечению безопасности информации в организации
5	Проверка физической защищенности информационных ресурсов - Проверка физической защищенности серверных комнат и других объектов - Оценка контроля доступа и мер по предотвращению несанкционированного доступа В результате выполнения работы студент получает практические навыки проверки физической защищенности информационных ресурсов, что поможет студентам оценить уровень физической безопасности серверных комнат и других объектов.
6	Проверка уровня защиты операционных систем и сетей - Анализ уровня защиты операционных систем и сетей - Оценка правильности настройки системы контроля доступа и аутентификации

№ п/п	Тематика практических занятий/краткое содержание
	В результате выполнения работы студент получает практические навыки проверки уровня защиты операционных систем и сетей, что позволит студентам оценить правильность настройки системы контроля доступа и аутентификации.
7	Проверка процессов управления доступом и привилегиями пользователей - Анализ процессов управления доступом и привилегиями - Оценка эффективности механизмов идентификации и аутентификации В результате выполнения работы студент получает практические навыки проверки процессов управления доступом и привилегиями пользователей, что поможет студентам оценить эффективность механизмов идентификации и аутентификации.
8	Проверка систем защиты информации от внешних атак - Анализ наличия и эффективности систем защиты от внешних атак - Оценка уровня обнаружения и предотвращения киберугроз В результате выполнения работы студент получает практические навыки проверки систем защиты информации от внешних атак, что поможет студентам оценить наличие и эффективность систем защиты от киберугроз.
9	Проверка мер по предотвращению утечки информации внутри организации - Анализ мер по предотвращению утечки информации внутри организации - Оценка эффективности систем мониторинга и обнаружения нарушений В результате выполнения работы студент получает практические навыки проверки мер по предотвращению утечки информации внутри организации, что поможет студентам оценить эффективность систем мониторинга и обнаружения нарушений.
10	Проверка уровня защиты приложений и программного обеспечения - Анализ уровня защиты приложений от взлома и эксплуатации уязвимостей - Оценка процессов разработки и тестирования безопасности приложений В результате выполнения работы студент получает практические навыки проверки уровня защиты приложений и программного обеспечения, что поможет студентам оценить уровень защиты приложений от взлома и эксплуатации уязвимостей.
11	Проверка готовности и эффективности процессов реагирования на инциденты - Анализ готовности и эффективности процессов реагирования на инциденты - Оценка процедур регистрации, анализа и устранения инцидентов В результате выполнения работы студент получает практические навыки проверки готовности и эффективности процессов реагирования на инциденты, что поможет студентам оценить процедуры регистрации, анализа и устранения инцидентов.
12	Проверка эффективности программ обучения и осведомленности сотрудников - Анализ эффективности программ обучения и осведомленности сотрудников - Оценка степени соблюдения правил и политик безопасности В результате выполнения работы студент получает практические навыки проверки эффективности программ обучения и осведомленности сотрудников, что поможет студентам оценить степень соблюдения правил и политик безопасности.
13	Проверка процессов документирования и архивирования информации - Анализ процессов документирования и архивирования информации - Оценка соответствия требованиям законодательства и политик безопасности В результате выполнения работы студент получает практические навыки проверки процессов документирования и архивирования информации, что поможет студентам оценить соответствие требованиям законодательства и политик безопасности.
14	Проведение аудита информационной безопасности в организации - Проведение аудита информационной безопасности в организации

№ п/п	Тематика практических занятий/краткое содержание
15	Подготовка отчета по результатам аудита информационной безопасности - Разработка отчета по результатам аудита информационной безопасности В результате выполнения работы студент получает практические навыки подготовки отчета по результатам аудита информационной безопасности, что поможет студентам научиться структурировать и представлять результаты аудита с рекомендациями для улучшения безопасности информации.
16	Подготовка отчета по результатам аудита информационной безопасности (продолжение) - Представление отчета и обсуждение рекомендаций с руководством организации В результате выполнения работы студент получает практические навыки подготовки отчета по результатам аудита информационной безопасности, что поможет студентам научиться структурировать и представлять результаты аудита с рекомендациями для улучшения безопасности информации.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом .
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	Козьминых, С. И. Аудит информационной безопасности : учебное пособие / С. И. Козьминых, С. А. Борисов. — Москва : КноРус, 2026. — 336 с. — ISBN 978-5-406-15552-3.	Текст : электронный // eLIBRARY.RU : [сайт]. — URL: https://www.elibrary.ru/item.asp?id=65638717 (дата обращения: 22.09.2026). — Режим доступа: для авторизир. пользователей
2	Скрыпников, А. В. Аудит информационной безопасности : учебное пособие / А. В. Скрыпников, В. В. Зиновьева, И. А. Саранов, А. А. Берестовой, В. Э. Меерсон ; науч. ред. А. В. Скрыпников ; Воронежский государственный университет инженерных технологий. — Воронеж : Воронежский государственный университет инженерных технологий, 2024.	Текст : электронный // eLIBRARY.RU : [сайт]. — URL: https://www.elibrary.ru/item.asp?id=83225197 (дата обращения: 22.09.2026). — Режим доступа: для авторизир. пользователей.

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

- 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).

- 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:

Зачет в 9 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