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 - программа бакалавриата
по направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудит информационной безопасности

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

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: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Цели и задачи изучения дисциплины «Аудит информационной безопасности» соотносятся с общими целями ГОС ВПО по специальности/направлению подготовки. Слушатель получает систематизированные теоретические и практические знания в области информационной безопасности. Целью изучения дисциплины является обучение современным технологиям в области информационных систем, создания и эксплуатации систем защиты информации.

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.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Эксплуатационная:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологическая:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

- проведение проектных расчетов элементов систем обеспечения информационной

безопасности;

- участие в разработке технологической и эксплуатационной документации;

- проведение предварительного технико-экономического обоснования проектных расчетов

Экспериментально-исследовательская деятельность:

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

- проведение экспериментов по заданной методике, обработка и анализ их результатов;

- проведение вычислительных экспериментов с использованием стандартных программных средств

Организационно-управленческая деятельность:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

- организация работы малых коллективов исполнителей;

- участие в совершенствовании системы управления информационной безопасностью;

- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;

- контроль эффективности реализации политики информационной безопасности объекта защиты.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1.4 - Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;

ПК-5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ;

ПК-10 - способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности .

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

Знать:

- стандарты по ИБ;
- порядок и стадии проведения аудита ИБ;
- принципы работы с информацией;
- основные угрозы информационной безопасности и методы защиты от них;
- основные нормативные документы, определяющие политику безопасности предприятия.

Уметь:

- анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ;
- использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры;
- применять эти методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ;
- ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ.

Владеть:

- способностью применять на практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации ИБ методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем

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 №8
Контактная работа при проведении учебных занятий (всего):	60	60
В том числе:		
Занятия лекционного типа	30	30
Занятия семинарского типа	30	30

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 48 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.

№ п/п	Тематика лекционных занятий / краткое содержание
5	Анализ угроз и уязвимостей информационной безопасности - Идентификация угроз и уязвимостей в информационной системе - Оценка рисков и определение приоритетов для проведения аудита.
6	Оценка соответствия политике информационной безопасности - Проверка соответствия политике и процедурам информационной безопасности - Анализ эффективности мер по обеспечению безопасности информации.
7	Аудит физической безопасности информационных ресурсов - Проверка физической защищенности серверных комнат, ЦОД и других объектов - Оценка контроля доступа и мер по предотвращению несанкционированного доступа.
8	Аудит логической безопасности информационных систем - Проверка уровня защиты операционных систем, сетей и баз данных - Оценка правильности настройки системы контроля доступа и аутентификации.
9	Аудит управления доступом к информационным ресурсам - Проверка процессов управления доступом и привилегиями пользователей - Оценка эффективности механизмов идентификации 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 - 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.

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.

№ п/п	Тематика практических занятий/краткое содержание
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 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

№ п/п	Тематика практических занятий/краткое содержание
	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
15	Подготовка отчета по результатам аудита информационной безопасности - Разработка отчета по результатам аудита информационной безопасности - 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	Аверченков В. И., Аудит информационной безопасности : учебное пособие / В. И. Аверченков. — 2-е изд. — Москва : ФЛИНТА, 2011. — 269 с. — ISBN 978-5-9765-1256-6.	Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/20195 (дата обращения: 01.03.2024).
2	Башлы П.Н., Информационная безопасность и защита информации : учебное пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К.. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7.	образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/10677.html (дата обращения: 01.03.2024). — Режим доступа: для авторизир. пользователей

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

Современные профессиональные базы данных и информационные справочные системы не требуются.

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

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть обеспечен лицензионными программными продуктами:

• Foxit Reader/Acrobat Reader

• Microsoft Office (Power Point)

Для проведения практических занятий необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:

• Foxit Reader/Acrobat Reader

• Microsoft Office (Word).

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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

- Для проведения аудиторных занятий требуется специализированная лекционная аудитория с мультимедиа аппаратурой.
- Для проведения практических работ: компьютеры с предустановленным Microsoft Windows не ниже Windows XP и процессором не ниже Pentium 4.

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Зачет в 8 семестре.

10. Оценочные материалы.

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

Авторы:

С.В. Антошкин

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической комиссии Н.А. Андриянова