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
20.04.01 Техносферная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Контроль и аудит систем безопасности

Направление подготовки: 20.04.01 Техносферная безопасность

Направленность (профиль): Гигиена и техносферные риски транспортных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Цель дисциплины «Контроль и аудит систем безопасности» — сформировать у обучающихся комплексные знания и практические навыки в области оценки, мониторинга и проверки эффективности систем безопасности (в т.?ч. информационной, транспортной, промышленной) для своевременного выявления уязвимостей, нарушений и рисков, а также обеспечения соответствия нормативным требованиям и стандартам. Задачи дисциплины включают: изучение нормативно?правовой базы в сфере безопасности; освоение методик проведения аудитов и инспекций; формирование навыков выявления и классификации угроз и уязвимостей; обучение разработке корректирующих мероприятий по устранению выявленных недостатков; отработку применения инструментов контроля и мониторинга систем безопасности; закрепление понимания процессов документирования результатов проверок и составления отчётности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-3 - Способность принимать участие в проектной деятельности транспортно- технологических комплексов.

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

Знать:

в рамках компетенции ПК-3 обучающийся должен знать основные принципы организации и управления проектной деятельностью в сфере транспортно-технологических комплексов, нормативно-правовую базу (включая требования ФГОС и отраслевые стандарты), методы оценки технических и технологических решений, а также типовые этапы жизненного цикла проекта — от постановки задачи до внедрения и мониторинга результатов.

Уметь:

обучающийся должен уметь участвовать в разработке проектных решений для транспортно-технологических систем, анализировать исходные данные и ограничения, применять методы моделирования и оптимизации технологических процессов, взаимодействовать в составе проектной

команды, а также обосновывать выбор технических решений с учётом требований безопасности и эффективности.

Владеть:

в части владения компетенцией ПК-3 предполагается владение инструментами проектного управления (в том числе цифровыми платформами и CAD-системами), навыками работы с технической документацией и стандартами, методами оценки рисков и обеспечения техносферной безопасности в проектных решениях, а также способностью адаптировать типовые проектные подходы к специфике транспортно-технологических комплексов.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 2 з.е. (72 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):	24	24
В том числе:		
Занятия лекционного типа	8	8
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 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	Лекция 1. Введение в контроль и аудит систем безопасности Понятие контроля и аудита в контексте систем безопасности. Цели, задачи и принципы проведения контроля и аудита. Виды контроля: государственный, ведомственный, общественный, внутренний. Роль аудита в обеспечении безопасности объектов и процессов. Нормативно-правовая база (ФЗ, ГОСТ, ISO, отраслевые стандарты).
2	Лекция 2. Нормативно?правовое регулирование контроля и аудита систем безопасности Обзор ключевых нормативных актов РФ в области безопасности (ФЗ «О безопасности», ФЗ «О транспортной безопасности» и др.). Международные стандарты: ISO 31000 (риск-менеджмент), ISO 27001 (информационная безопасность), ISO 45001 (охрана труда). Требования отраслевых регуляторов (Ростехнадзор, ФСБ, МВД и т. д.). Ответственность за несоблюдение требований безопасности.
3	Лекция 3. Методология аудита систем безопасности Основные этапы проведения аудита: планирование, подготовка, проведение, оформление результатов. Методы сбора информации: интервью, опросы, наблюдение, анализ документов. Инструменты аудита: чек-листы, анкеты, матрицы рисков. Критерии оценки соответствия систем безопасности нормативным требованиям. Особенности внутреннего и внешнего аудита.
4	Лекция 4. Виды и методы контроля систем безопасности Классификация видов контроля: предварительный, текущий, заключительный; плановый и внеплановый. Технические методы контроля: инструментальные замеры, испытания, мониторинг. Организационные методы: проверки документации, инструктажи, тренировки. Автоматизированные системы контроля (СКУД, видеонаблюдение, датчики). Принципы риск-ориентированного контроля.

№ п/п	Тематика лекционных занятий / краткое содержание
5	Лекция 5. Аудит информационной безопасности Угрозы информационной безопасности на предприятии. Аудит ИТ-инфраструктуры: сети, серверы, рабочие станции. Оценка защищённости данных (персональных, коммерческой тайны). Проверка соответствия требованиям 152-ФЗ, 187-ФЗ, PCI DSS. Анализ политик ИБ, журналов событий, настроек безопасности.
6	Лекция 6. Аудит промышленной и экологической безопасности Контроль соблюдения норм промышленной безопасности на опасных производственных объектах. Аудит систем охраны труда: оценка условий труда, СИЗ, инструктажей. Экологический аудит: воздействие на окружающую среду, отходы, выбросы. Проверка систем противоаварийной защиты и локализации аварий. Документирование результатов и разработка корректирующих мероприятий.
7	Лекция 7. Аудит транспортной безопасности Нормативная база транспортной безопасности (ФЗ 16, приказы Минтранса). Аудит объектов транспортной инфраструктуры (вокзалы, аэропорты, мосты). Оценка мер по защите от актов незаконного вмешательства. Проверка работы систем видеонаблюдения, досмотра, контроля доступа. Анализ планов обеспечения транспортной безопасности.
8	Лекция 8. Процедуры проведения аудита и оформление результатов Подготовка к аудиту: составление программы, чек-листов, графика. Проведение аудита: сбор данных, фиксация несоответствий. Оформление отчёта: структура, обязательные разделы, выводы. Рекомендации по устранению выявленных нарушений. Согласование результатов с руководством и разработка плана корректирующих действий.
9	Лекция 9. Мониторинг и контроль исполнения рекомендаций по итогам аудита Организация системы мониторинга устранения нарушений. Периодичность проверок исполнения корректирующих мероприятий. Оценка эффективности внедрённых мер. Ведение реестра рисков и несоответствий. Цикличность процесса: аудит > корректировка > повторный аудит.

№ п/п	Тематика лекционных занятий / краткое содержание
10	Лекция 10. Современные тенденции и технологии в контроле и аудите систем безопасности Цифровые инструменты аудита: мобильные приложения, облачные платформы, BI-аналитика. Использование Big Data и ИИ для прогнозирования рисков. IoT-датчики для непрерывного мониторинга параметров безопасности. Внедрение риск-ориентированных моделей контроля. Перспективы развития аудита систем безопасности в условиях цифровизации.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Занятие 1. Анализ нормативно?правовой базы в сфере безопасности Изучение ключевых федеральных законов (ФЗ «О безопасности», ФЗ «О транспортной безопасности» и др.). Работа с международными стандартами (ISO 31000, ISO 27001). Составление таблицы нормативных актов по сферам применения (промышленная, информационная, транспортная безопасность). Определение требований к объектам конкретного типа.
2	Занятие 2. Разработка программы аудита безопасности Составление плана аудита для условного предприятия. Формулировка целей и задач проверки. Выбор методов сбора данных (интервью, наблюдение, анализ документов). Разработка чек-листов для разных направлений аудита (охрана труда, ИБ, пожарная безопасность).
3	Занятие 3. Проведение имитационного аудита информационной безопасности Моделирование угроз ИБ для ИТ-инфраструктуры организации. Проверка настроек безопасности серверов и рабочих станций. Анализ политик доступа и парольной политики. Оформление промежуточного отчёта с выявленными уязвимостями.
4	Занятие 4. Аудит промышленной безопасности опасного производственного объекта Оценка соответствия объекта требованиям Ростехнадзора. Проверка документации по охране труда и промышленной безопасности.

№ п/п	Тематика практических занятий/краткое содержание
	Анализ журналов инструктажей и проверок СИЗ. Выявление нарушений и их классификация по степени риска.
5	Занятие 5. Оценка транспортной безопасности на примере автовокзала Аудит систем видеонаблюдения, контроля доступа и досмотра. Проверка планов обеспечения транспортной безопасности. Моделирование сценария акта незаконного вмешательства. Разработка рекомендаций по усилению защиты объекта.
6	Занятие 6. Расчёт и анализ рисков с использованием матрицы рисков Идентификация опасностей на условном предприятии. Оценка вероятности и тяжести последствий для каждой угрозы. Построение матрицы рисков (низкий/средний/высокий уровень). Приоритизация мер по снижению наиболее критических рисков.
7	Занятие 7. Оформление отчёта по результатам аудита Структура отчёта: введение, методология, результаты, выводы, рекомендации. Практическое заполнение разделов на основе данных имитационного аудита. Формулировка корректирующих мероприятий с указанием сроков и ответственных. Согласование проекта отчёта с «руководством» (в рамках деловой игры).
8	Занятие 8. Мониторинг исполнения корректирующих мероприятий Создание реестра выявленных нарушений и рекомендаций. Разработка графика контрольных проверок. Отработка методики оценки эффективности внедрённых мер. Заполнение формы мониторинга устранения несоответствий.
9	Занятие 9. Использование цифровых инструментов для аудита и контроля Ознакомление с мобильными приложениями для фиксации нарушений (фото, геотеги). Работа с облачными платформами для сбора и анализа данных. Визуализация результатов аудита с помощью BI-систем (Power BI, Tableau). Практический разбор кейса с применением IoT-датчиков для мониторинга параметров безопасности.
10	Занятие 10. Деловая игра «Аудит комплексной системы безопасности предприятия» Распределение ролей: аудиторы, представители подразделений, руководство. Проведение комплексного аудита по направлениям (ИБ, охрана труда, экологическая безопасность).

№ п/п	Тематика практических занятий/краткое содержание
	Подготовка итогового отчёта и презентация результатов перед «комиссией». Обсуждение стратегии долгосрочного управления рисками на предприятии.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к промежуточному контролю
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.

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

№ п/п	Библиографическое описание	Место доступа
1	Системы безопасности автомобилей Савич Евгений Леонидович, Капустин Владимир Владимирович Учебное пособие НИЦ ИНФРА-М , 2024	https://znanium.ru/catalog/document?id=435081
2	Интегрированные системы безопасности Карабанов Ростислав Михайлович Учебное пособие Владимирский юридический институт ФСИН России , 2023	https://znanium.ru/catalog/document?id=446638

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

1. Электронная библиотека РУТ (МИИТ) http://library.miit.ru/
2. Электронно-библиотечная система «Лань» https://e.lanbook.com/
3. Образовательная платформа «Юрайт» https://urait.ru/
4. Электронно-библиотечная система «ZNANIUM» https://znanium.com/
5. Научная электронная библиотека eLibrary https://elibrary.ru/
6. База данных PubMed (медико-биологические исследования) https://pubmed.ncbi.nlm.nih.gov/
7. Scopus / Web of Science (доступ через подписку ВУЗа).
8. Электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/

9. Справочно-правовая система «КонсультантПлюс» (доступ из сети ВУЗа).

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

SearchInform КИБ — защита от утечек информации, перехват сообщений, аудит действий пользователей, контроль коммуникаций.

InfoWatch Traffic Monitor — анализ и блокировка утечек конфиденциальной информации, контроль каналов передачи данных.

Forcepoint DLP — защита данных в корпоративной сети и за её пределами, контроль USB?устройств, облачных сервисов, SSL?трафика.

Стахановец — DLP?система с биометрической аутентификацией, контроль копирования данных, блокировка скриншотов экрана, мониторинг мессенджеров и почты.

Гарда Предприятие — анализ передаваемой информации, блокировка отправки секретных файлов, мониторинг сетевого трафика без установки агентов.

ИНСАЙДЕР — контроль коммуникаций персонала, фиксация скриншотов, кейлоггинг, анализ активности сотрудников.

Perimetrix — маркировка и контроль жизненного цикла корпоративных данных, управление правами доступа к файлам

AlienVault (AT&T Cybersecurity) — комплексная диагностика, обнаружение угроз, автоматический анализ журналов, оповещения по email.

Rapid7 InsightIDR — выявление инцидентов, реагирование на несанкционированный доступ, поиск и устранение угроз.

Sumo Logic — интеллектуальный анализ безопасности, управление журналами, устранение угроз в реальном времени.

ManageEngie EventLog Analyzer — мониторинг веб?серверов, баз данных и почтовых служб, оповещения о несанкционированном доступе.

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

Учебные аудитории для лекционных и практических занятий, оснащенные мультимедийным оборудованием (проектор, экран, компьютер).

• Компьютерный класс с доступом в интернет для проведения практических занятий, поиска информации в базах данных, выполнения расчетов.

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:

ассистент кафедры «Управление безопасностью в техносфере» Р.Л. Кудрявцева

Согласовано:

Заведующий кафедрой ГТ М.Ф. Вильк

Председатель учебно-методической комиссии Н.А. Андриянова