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 РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудит информационной безопасности компьютерных систем железнодорожного транспорта

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины (модуля) «Аудит информационной безопасности компьютерных систем железнодорожного транспорта» являются изучение методов и средств управления информационной безопасностью (ИБ) на объекте и изучение основных подходов к разработке, реализации, анализу сопровождению и совершенствованию систем управления информационной безопасности (СУИБ) компьютерных систем железнодорожного транспорта.

Задачей дисциплины является формирование у обучающихся профессиональных компетенций в области организации и проведения аудита информационной безопасности, необходимых для обеспечения эффективного функционирования, контроля и постоянного совершенствования системы управления информационной безопасностью (СУИБ) компьютерных систем железнодорожного транспорта.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-6 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ПК-7 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации.

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

Знать:

- Состав организационных и технических мер защиты информации согласно нормативным документам (Приказы ФСТЭК №17, №21, №31).
- Современные и перспективные математические методы (криптографические, стеганографические, методы теории кодирования), используемые при построении средств защиты.
- Нормативно-правовую базу РФ в области защиты информации (ФЗ №149, ФЗ №152, ГОСТы, Приказы ФСТЭК и ФСБ).
- Классификацию угроз безопасности информации (по природе возникновения, по направленности, по источникам).

- Виды и методы тестирования систем защиты (функциональное, нагрузочное, на проникновение, статический и динамический анализ кода).

- Перечень необходимых документов на этапе эксплуатации АС (формуляр, руководство оператора, руководство администратора, инструкция пользователю по безопасности).

- Критерии и показатели эффективности защиты информации (вероятность предотвращения атаки, время восстановления, полнота регистрации событий).

- Требования законодательства о защите информации применительно к деятельности организации.

Уметь:

- Определять ресурсы (трудовые, финансовые, технические), необходимые для реализации плана.

- Анализировать техническую документацию и проводить тестирование (бенчмаркинг) программно-аппаратных средств для выявления их соответствия заявленным характеристикам.

- Формулировать технико-экономическое обоснование (ТЭО) необходимости внедрения средств и мер защиты.

- Составлять полный перечень возможных угроз, актуальных для конкретной АС, с учетом ее архитектуры и особенностей функционирования.

- Проводить тестовые воздействия, имитирующие действия нарушителя, и проверять корректность реагирования СЗИ.

- Описывать действия персонала по настройке, администрированию и контролю работоспособности СЗИ.

- Выявлять "узкие места" в системе защиты и причины снижения ее эффективности.

- Разрабатывать проекты документов, регламентирующих обработку и защиту информации (в т.ч. персональных данных).

Владеть:

- Навыками работы с математическим аппаратом, лежащим в основе работы средств защиты (например, вычисление хэш-функций, проверка ЭП).

- Навыками составления аналитических записок и обосновывающих документов для руководства.

- Навыками использования специализированного ПО для сканирования уязвимостей и анализа защищенности.

- Навыками работы с современными программными и программно-аппаратными комплексами тестирования.

- Методами унификации и стандартизации при разработке документов.

- Методами оценки трудоемкости и стоимости этапов работ по созданию СЗИ.

- Навыками работы с системами сбора и корреляции событий (SIEM).

- Методами анализа действующей документации на предмет ее полноты и непротиворечивости.

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):	48	48
В том числе:		
Занятия лекционного типа	32	32
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 96 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 Рассматриваемые вопросы: - Важность и актуальность дисциплины. - Ее взаимосвязь с другими дисциплинами специальности. - Содержание дисциплины. - Виды контроля знаний
2	Базовые вопросы управление ИБ Рассматриваемые вопросы: - Цели и задачи управления ИБ. - Понятие системы управления. - Понятие СУИБ. - Место СУИБ в рамках общей системы управления предприятием
3	Нормативно законодательная база обеспечения безопасности в рамках СУИБ Рассматриваемые вопросы: - Нормативно-законодательные документы РФ по обеспечению ИБ. - Её анализ и структура
4	Основные стандарты, регламентирующие управление ИБ Рассматриваемые вопросы: - Существующие стандарты и методологии по управлению ИБ. - Сравнительный анализ на примере стандартов.
5	Процессный подход Рассматриваемые вопросы: - Понятие процесса. - Методы формализации процессов. - Понятие процессорного подхода. - Процессорный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). - Основные процессы СУИБ
6	Ролевая структура СУИБ Рассматриваемые вопросы: - Понятие роли. - Использование ролевого принципа в рамках СУИБ, его преимущества. - Ролевая структура СУИБ (основные и дополнительные роли). - Роль высшего руководства организации (компании) в СУИБ. - Этапы разработки и функционирования СУИБ
7	Политика СУИБ Рассматриваемые вопросы: - Понятие политики СУИБ. - Цели и задачи политики СУИБ. - Структура и содержание Политики СУИБ. - Источники информации для разработки политики СУИБ.
8	Процессы анализа рисков ИБ Рассматриваемые вопросы: - Цели процесса анализа рисков ИБ. - Этапы и участники процесса анализа риской ИБ. - Разработка методики анализа рисков ИБ. - Инвентаризация активов. - Источники информации об активах организации
9	Выбор угроз ИБ и уязвимости для выделенных активов. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Оценка рисков ИБ. - Планирование мер по обработке выявленных рисков ИБ. - Результаты анализа рисков ИБ и рекомендации по их применению.
10	Основные процессы СУИБ Рассматриваемые вопросы: - Процессы «управления документами» и «управление записями». - Цели и задачи процессов. - Входные и выходные данные. - Обязательные этапы процессов, связи с другими процессами СУИБ.
11	Процессы совершенствования СУИБ Рассматриваемые вопросы: - Процессы совершенствования СУИБ («внутренний аудит», «корректирующие действия», «предупреждающие действия»). - Процесс «Мониторинг эффективности»
12	Внедрение разработанных процессов Рассматриваемые вопросы: - Этапы внедрения процессов и их последовательность. - Особенности и сложности внедрения процессов управления ИБ. - Способы их решения. - Контроль внедрения процессов. - Документирование процесса внедрения разработанных процессов. - Типовой документ «Положение о применимости документа. - Процесс разработки документа.
13	Процесс управления инциндентами ИБ Рассматриваемые вопросы: - Цели и задачи процесса «Управление инцидентами ИБ». - Входные и выходные данные процесса. - Обязательные этапы процесса. - Связи с другими процессами СУИБ.
14	Независимы аудит СУИБ Рассматриваемые вопросы: - Внешний аудит ИБ на соответствие требованиям нормативных документов. - Этапы проведения аудита. - Результаты аудита и их интеграция.
15	Эксплуатация СУИБ Рассматриваемые вопросы: - Ввод системы в эксплуатацию. - Возможные проблемы и способы их решения. - Приемо-сдаточные испытания - Период эксплуатации СУИБ перед сертификацией
16	Сертификация аудита Рассматриваемые вопросы: - Сертификация по ISO/IEC 2700 (или ГОСТ РИСО/МЭК 27001). - Этапы сертификационного аудита. - Решение о сертификации.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Система управления ИБ конкретного объекта информатизации В результате выполнения лабораторной работы студент отрабатывает умение формирования требований к системе управления ИБ конкретного объекта информатизации
2	Проектирование СУИБ В результате выполнения работы студент отрабтывает умение по проектированию СУИБ конкретного объекта информатизации
3	Защита компакт-дисков от копирования В результате выполнения лабораторной работы студент рассматривает регламент обеспечения защиты компакт-дисков от копирования
4	Риски для СУИБ В результате работы студент отрабатывает применение методов анализа рисков для СУИБ
5	Управление документами В результате выполнения работы студент отрабатывает умение моделировать процессы "управления документами".
6	Эффективность СУИБ В результате выполнения работы студент рассматривает основные примеры совершенствования и мониторинг эффективности СУИБ.
7	Управление СУИБ В результате выполнения работы студент получает навык внедрения процессов управления СУИБ.
8	Положение о применимости В результате выполнения работы студент отрабатывает умение разрабатывать импового документа "Положение о применимости"
9	Аудит СУИБ. В результате выполнения работы студент применяет особенности внешнего аудита СУИБ.
10	Этапы аудита СУИБ В результате выполнения работы студент отрабатывает умение по разработки этапов проведения аудита СУИБ
11	Результаты аудита СУИБ В результате выполнения лабораторной работы студент отрабатывает умение по обработке результатов аудита СУИБ.
12	СУИБ конкретного объекта информатизации В результате выполнения работы студент отрабатывает умение разрабатывать политику СУИБ конкретного объекта информатизации
13	СУИБ по стандарту ГОСТ Р ИСО/МЭК 27001 В результате выполнения работы студент рассматривает практику сертификации СУИБ по стандарту ГОСТ Р ИСО/МЭК 27001

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к лабораторным работам.
3	Выполнение курсового проекта.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

Тематика предлагаемых курсовых проектов:

1) Модели управления инцидентами информационной безопасности

2) Аудит информационной безопасности баз данных и систем управления базами данных

3) Основы построения защищенных компьютерных сетей

4) Анализ проблем управления инцидентами ИБ компании

5) Модели управления инцидентами ИБ

6) Построение процесса управления инцидентами компании ИБ

7) Анализ и выбор инструментальных средств для создания подсистемы управления инцидентами организации ИБ

8) Верификационный подход к оценке и управлению рисками

9) Риск-ориентированный подход к оценке и управления рисками

10) Аудит ИБ КС и необходимость его применения

11) Комплексный аудит ИБ и его возможности

12) Внешний аудит ИБ организаций и его применение

13) Внутренний аудит ИБ и технология его применения

14) Программа проведения аудита ИБ, ее основные компоненты и этапы

15) Тесты на проникновения и необходимость их применения

16) Аудит ИБ пользователей КС компании

17) Аудит информационной безопасности средств телекоммуникации и средств связи

18) Анализ систем обнаружения атак компании CISCO

19) Стандарты и нормативные документы по управлению инцидентами ИБ

20) Технология проведения комплексного аудита ИБ КС

21) Процесс управления инцидентами ИБ компаний

22) Инструментальные средства процесса расследования инцидентов ИБ компьютерных систем

23) Тестирование на проникновение как часть мероприятий по оценке защищенности сети

24) Анализ методов и средств тестирования на проникновение в КС

25) Аудит ИБ СУБД и БД на основе Oracle

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

№ п/п	Библиографическое описание	Место доступа
1	Информационное право Леонтьев А.Н. Учебное пособие Волг-ГТУ. - Волгоград, - 76 с. - ISBN 978-5-9948-3293-6 , 2019	https://reader.lanbook.com/book/157203#3
2	Организационное и правовое обеспечение информационной безопасности: Крыжановский А.В. Методические указания Самара: ПГУТИ, - 56 с. , 2018	https://reader.lanbook.com/book/182279#2

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/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

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

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Операционная система Lunix

Пакет программ SysInternalsSuite

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 9 семестре.
Курсовой проект в 9 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, профессор, д.н. кафедры "Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах" Института железнодорожного транспорта М.Я. Клепцов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин