

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

26 мая 2020 г.


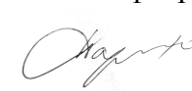
Кафедра «Управление и защита информации»

Автор Клепцов Михаил Яковлевич, д.т.н., профессор

**АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ**

**«Аудит информационной безопасности компьютерных систем  
железнодорожного транспорта»**

Специальность:	<u>10.05.01 – Компьютерная безопасность</u>
Специализация:	<u>Информационная безопасность объектов информатизации на базе компьютерных систем</u>
Квалификация выпускника:	<u>Специалист по защите информации</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2020</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">С.В. Володин</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 16 21 мая 2020 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
---	--

Москва 2020 г.

## 1. Цели освоения учебной дисциплины

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 безопасностью (СУИБ) компьютерных систем железнодорожного транспорта.

## 2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Аудит информационной безопасности компьютерных систем железнодорожного транспорта" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

## 3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПКР-5	Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации
ПКР-8	Способен подготовить обоснование необходимости защиты информации в автоматизированной системе
ПКР-9	Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой
ПКР-10	Способен проводить тестирование систем защиты информации автоматизированных систем
ПКР-11	Способен участвовать в разработке эксплуатационной документации на системы защиты информации автоматизированных систем
ПКС-2	Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
ПКС-3	Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
ПКС-5	Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации

## 4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

## 5. Образовательные технологии

Преподавание дисциплины «Аудит информационной безопасности компьютерных систем железнодорожного транспорта» осуществляется в форме лекций и практических занятий. В соответствии с требованиями ФГОС ВО по направлению 10.05.01 «Компьютерная безопасность» с целью формирования и развития профессиональных навыков студентов предусмотрено использовать и проводить разбор презентаций лучших

дипломных проектов по данной специализации. Кроме того, предусмотрены мастер-классы специалистов из:- академии ФСБ- компании «Информзащита»- лаборатории Касперского- РОСАТОМА.

## **6. Содержание дисциплины (модуля), структурированное по темам (разделам)**

### **РАЗДЕЛ 1**

Введение

Тема: Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний

### **РАЗДЕЛ 2**

Базовые вопросы управление ИБ

Тема: Цели и задачи управления ИБ. Понятие системы управления.

Тема: Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием

### **РАЗДЕЛ 3**

Нормативно законодательная база обеспечения безопасности в рамках СУИБ

Тема: Нормативно-законодательные документы РФ по обеспечению ИБ.

Тема: Её анализ и структура

### **РАЗДЕЛ 4**

Основные стандарты, регламентирующие управление ИБ

Тема: Существующие стандарты и методологии по управлению ИБ.

Тема: Сравнительный анализ на примере стандартов.

### **РАЗДЕЛ 5**

Процессный подход

Тема: Понятие процесса. Методы формализации процессов. Понятие процессорного подхода.

Тема: Процессорный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Основные процессы СУИБ

### **РАЗДЕЛ 6**

Ролевая структура СУИБ

Тема: Понятие роли. Использование ролевого принципа в рамках СУИБ, его преимущества.

Тема: Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации (компании) в СУИБ. Этапы разработки и функционирования СУИБ

### **РАЗДЕЛ 7**

Политика СУИБ

Тема: Понятие политики СУИБ. Цели и задачи политики СУИБ.

Тема: Структура и содержание Политики СУИБ. Источники информации для разработки политики СУИБ.

## РАЗДЕЛ 8

### Процессы анализа рисков ИБ

Тема: Цели процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка методики анализа рисков ИБ. Инвентаризация активов. Источники информации об активах организации

Тема: Выбор угроз ИБ и уязвимости для выделенных активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Результаты анализа рисков ИБ и рекомендации по их применению.

## РАЗДЕЛ 9

### Основные процессы СУИБ

Текущий контроль РИТМ (тестирование, устный/письменный опрос)

Тема: Процессы «управления документами» и «управление записями». Цели и задачи процессов. Входные и выходные данные. Обязательные этапы процессов, связи с другими процессами СУИБ.

Тема: Процессы совершенствования СУИБ («внутренний аудит», «корректирующие действия», «предупреждающие действия»). Процесс «Мониторинг эффективности»

## РАЗДЕЛ 10

### Внедрение разработанных процессов

Тема: 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.

## РАЗДЕЛ 11

### Процесс управления инцидентами ИБ

Тема: Цели и задачи процесса «Управление инцидентами ИБ».

Тема: Входные и выходные данные процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

## РАЗДЕЛ 12

### Независимы аудит СУИБ

Тема: Внешний аудит ИБ на соответствие требованиям нормативных документов.

Тема: Этапы проведения аудита.

Тема: Результаты аудита и их интеграция.

## РАЗДЕЛ 13

### Эксплуатация СУИБ

Текущий контроль РИТМ (тестирование, устный/письменный опрос)

Тема: Ввод системы в эксплуатацию. Возможные проблемы и способы их решения.

Тема: Приемо-сдаточные испытания

Тема: Период эксплуатации СУИБ перед сертификацией

#### РАЗДЕЛ 14

Сертификация аудита

Тема: Сертификация по ISO/IEC 2700 (или ГОСТ Р ИСО/МЭК 27001). Этапы сертификационного аудита. Решение о сертификации.

#### РАЗДЕЛ 15

Курсовой проект

#### РАЗДЕЛ 16

Зачет с оценкой