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 - программы специалитета
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

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

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.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-17 - Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации;

ПК-20 - Способен подготовить обоснование необходимости защиты информации в автоматизированной системе;

ПК-21 - Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой;

ПК-22 - Способен проводить тестирование систем защиты информации автоматизированных систем;

ПК-23 - Способен участвовать в разработке эксплуатационной документации на системы защиты информации автоматизированных систем;

ПК-25 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-26 - Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-28 - 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.

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

Уметь:

Проводит сравнительный анализ программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

Уметь:

Делает обоснованный выбор программно-аппаратных средств защиты информации.

Уметь:

Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта.

Уметь:

Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.

Владеть:

Проводит анализ угроз безопасности информации, обрабатываемой автоматизированными системами высокоскоростного транспорта.

Уметь:

Проводит анализ угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.

Уметь:

Проводит индивидуальное тестирование систем защиты информации в блоке автоматизированных систем.

Знать:

Участвует в разработке эксплуатационной документации системы защиты информации в автоматизированных системах высокоскоростного транспорта.

Знать:

Участвует в разработке эксплуатационной документации на системы защиты информации в беспилотных автоматизированных системах.

Знать:

Знать основные процессы проектирования систем обеспечения информационной безопасности.

Уметь:

Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.

Уметь:

Уметь применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации.

Владеть:

Владеть навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.

Уметь:

Уметь разрабатывать нормативно правовые акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования.

Знать:

Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации.

Владеть:

Владеть навыками разработки нормативной правовой документации

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	Сем. №9
Контактная работа при проведении учебных занятий (всего):	50	50
В том числе:		

Занятия лекционного типа	34	34
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 94 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
2	Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний
3	Базовые вопросы управление ИБ
4	Цели и задачи управления ИБ. Понятие системы управления.
5	Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием
6	Нормативно законодательная база обеспечения безопасности в рамках СУИБ
7	Нормативно-законодательные документы РФ по обеспечению ИБ.
8	Её анализ и структура
9	Основные стандарты, регламентирующие управление ИБ
10	Существующие стандарты и методологии по управлению ИБ.
11	Сравнительный анализ на примере стандартов.
12	Процессный подход
13	Понятие процесса. Методы формализации процессов. Понятие процессорного подхода.

№ п/п	Тематика лекционных занятий / краткое содержание
14	Процессорный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Основные процессы СУИБ
15	Ролевая структура СУИБ
16	Понятие роли. Использование ролевого принципа в рамках СУИБ, его преимущества.
17	Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации (компании) в СУИБ. Этапы разработки и функционирования СУИБ
18	Политика СУИБ
19	Понятие политики СУИБ. Цели и задачи политики СУИБ.
20	Структура и содержание Политики СУИБ.Источники информации для разработки политики СУИБ.
21	Процессы анализа рисков ИБ
22	Цели процесса анализа рисков ИБ. Этапы и участники процесса анализа риской ИБ. Разработка методики анализа рисков ИБ. Инвентаризация активов. Источники информации об активах организации
23	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.
24	Основные процессы СУИБ
25	Процессы «управления документами» и «управление записями». Цели и задачи процессов. Входные и выходные данные. Обязательные этапы процессов, связи с другими процессами СУИБ.
26	Процессы совершенствования СУИБ («внутренний аудит», «корректирующие действия», «предупреждающие действия»). Процесс «Мониторинг эффективности»
27	Внедрение разработанных процессов
28	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.
29	Процесс управления инциндентами ИБ
30	Цели и задачи процесса «Управление инцидентами ИБ».
31	Входные и выходные данные процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.
32	Независимы аудит СУИБ
33	Внешний аудит ИБ на соответствие требованиям нормативных документов.
34	Этапы проведения аудита.
35	Результаты аудита и их интеграция.

№ п/п	Тематика лекционных занятий / краткое содержание
36	Эксплуатация СУИБ
37	Ввод системы в эксплуатацию. Возможные проблемы и способы их решения
38	Приемо-сдаточные испытания
39	Период эксплуатации СУИБ перед сертификацией
40	Сертификация аудита
41	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	ЛР1 Формирование требований к системе управления ИБ конкретного объекта информатизации
2	ЛР2 Проектирование СУИБ конкретного объекта информатизации
3	ЛР3 Регламент обеспечения защиты компакт-дисков от копирования
4	ЛР4 Применение методов анализа рисков для СУИБ
5	ЛР5 Применение методов анализа рисков для СУИБ
6	ЛР6 Моделирование процессов "управления документами".
7	ЛР7 Примеры совершенствования и мониторинг эффективности СУИБ.
8	ЛР8 Внедрение процессов управления СУИБ.
9	ЛР9 Процесс разработки импового документа "Положение о применимости"
10	ЛР10 Процесс разработки типового документа "Положение о применимости"
11	ЛР11 Применение внешнего аудита СУИБ.
12	ЛР12 Разработка этапов проведения аудита СУИБ
13	ЛР13 Обработка результатов аудита СУИБ.
14	ЛР14 Разработка политики СУИБ конкретного объекта информатизации
15	ЛР15 Разработка политики СУИБ конкретного объекта информатизации

№ п/п	Наименование лабораторных работ / краткое содержание
16	ЛР16 Разработка политики СУИБ конкретного объекта информатизации
17	ЛР17 Практика сертификации СУИБ по стандарту ГОСТ Р ИСО/МЭК 27001

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ
2	СР2 Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ
3	СР3 Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ, обеспечение безопасности в рамках СУИБ, обеспечение соответствия требованиям законодательства
4	СР4 Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ, обеспечение безопасности в рамках СУИБ, обеспечение соответствия требованиям законодательства
5	СР5 Мониторинг эффективности мер по обеспечению ИБ и процессов управления ИБ
6	СР6 Процессы совершенствования системы управления ИБ. Основные процессы и их взаимосвязь в рамках СУИБ
7	СР7 Процессы совершенствования системы управления ИБ. Основные процессы и их взаимосвязь в рамках СУИБ Внешний аудит ИБ. Цели и задачи. Методика проведения. Отчетность и рекомендации
8	Выполнение курсового проекта.
9	Подготовка к промежуточной аттестации.
10	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	Информационные системы и технологии управления Под ред. Г.А. Титоренко Книга ЮНИТИ-ДАНА , 2011	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)
2	Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга Издательский центр "Академия" , 2011	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)
1	Теория государственного и муниципального управления С.Ю. Наумов ФОРУМ , 2011	
2	Аудит информационной безопасности Под ред. А.П. Курило М., БДЦ-Пресс , 2006	
3	Правовое обеспечение информационной безопасности В.А. Минаев, А.П. Фисун М., Академия , 2008	
4	Политика информационной безопасности С.А. Петренко,В.А. Курбатов М., ДМК-Прессс , 2008	
5	Организационное обеспечение информационной безопасности О.А. Романов,С.А. Бабин, С.Г. Жданов М., Академия , 2008	

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

Не требуется

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

Операционная система семейства Microsoft Windows, на 2-5 компьютерах должна быть установлена серверная версия - Операционная система Lunix - Пакет программ SysInternalsSuite

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

Организация рабочего места студента в университете контролируется администрацией учебного заведения. Для лекций и практических занятий имеется компьютерный класс (локальная сеть, состоящая из 20 рабочих мест (компьютеров), сервера, компьютера преподавателя, проектора, электронная доска). Программное обеспечение не предусмотрено.

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 «Управление и защита информации»	Клепцов Михаил Яковлевич

Лист согласования

Заведующий кафедрой УиЗИ	Л.А. Баранов
Председатель учебно-методической комиссии	С.В. Володин