**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 бакалавриата
по направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором 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

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 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 | Сем. №8 |
| Контактная работа при проведении учебных занятий (всего): | 48 | 48 |
| В том числе: | | |
| Занятия лекционного типа | 24 | 24 |
| Занятия семинарского типа | 24 | 24 |

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 24 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 | 1. Основные понятия.<br>Описываются основные понятия, цели и задачи проведения аудита ИБ. Определяются моменты, когда необходимо проводить аудит, периодичность.<br><br>2. Виды, этапы и направления деятельности.<br>Рассматриваются виды и этапы проведения аудита. Описываются направления проведения аудита: первичный аудит; технический аудит, контрольный аудит.<br><br>3. Правовая база проведения аудита<br>Рассматриваются правовые и законодательные акты по проведению аудита |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | 4. Стандарты проведения аудита<br>Рассматривается структура международных и национальных стандартов в сфере аудита. Изучаются стандарт PCI DSS и методика их применения для оценки и управления безопасностью информационных технологий.<br>Рассматривается структура международных и национальных стандартов в сфере аудита. Изучаются стандарт ГОСТ Р 57580.1,и методика их применения для оценки и управления безопасностью информационных технологий.<br><br>5. Стадии и методика проведения аудита.<br>Рассматривается структура международных и национальных стандартов в сфере аудита. Изучаются стандарт ГОСТ Р 57580.1,и методика их применения для оценки и управления безопасностью информационных технологий.<br><br>6. Подготовка к аудиту ИБ.<br>Описываются состав и роли участников, порядок, цель и методы сбора исходной информации. Общие исходные данные. Исходные данные об обрабатываемой информации. Исходные данные о системе обеспечения безопасности информации. Исходные данные о персонале. Сбор дополнительных исходных данных.<br><br>7. Планирование аудита.<br>Описывается процесс инициирования процедуры аудита его цель, объект обследования. Рассматриваются критерии оценки значимости информационных ресурсов и процессов обработки информации. Описывается порядок и форма представления отчетов.<br><br>8. Моделирование угроз и тестирование<br>Рассматриваются цели и направления проведения моделирования. Описываются цели, методы и порядок проведения тестирования. Требования к размещению и использованию оборудования. Испытания функционирования системы защиты от НСД и защиты от утечки по техническим каналам. Тестирование рабочих станций (АРМ), серверов, межсетевых экранов, активного сетевого оборудования.<br><br>9. Документирование этапов проведения аудита ИБ.<br>Рассматриваются рекомендации по документированию: цель и методы обследования, проверка организационно-распорядительных документов, документирование результатов. |

## 4.2. Занятия семинарского типа.

### Практические занятия

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 1 | 1. Аудит информационной безопасности.<br>Виды, этапы и направления деятельности.<br>В результате выполнения работы студент получает практические навыки анализа требований документации.<br><br>2. Нормативно-правовая база проведения аудита ИБ.<br>Правовая база проведения аудита.<br>В результате выполнения работы студент получает практические навыки анализа нормативно правовой базы базы аудита информационной безопасности и ознакомиться с современными |

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| | методиками аудита ИБ.<br><br>3. Нормативно-правовая база проведения аудита ИБ.<br>Стандарты проведения аудита.<br>В результате выполнения работы студент получает практические навыки анализа нормативно правовой базы базы аудита информационной безопасности и ознакомиться с современными методиками аудита ИБ.<br><br>4. Методика и порядок проведения аудита ИБ.<br>Подготовка к аудиту ИБ.<br>Планирование аудита.<br>В результате выполнения работы студент получает практические навыки пранирования этапов аудита, анализа сроков и навыки в будущей профессиональной деятельности.<br><br>5. Методика и порядок проведения аудита ИБ.<br>Моделирование угроз и тестирование.<br>В результате выполнения работы студент получает практические навыки построения составления отчетности внутреннего аудита.<br><br>6. Методика и порядок проведения аудита ИБ.<br>Документирование этапов проведения аудита ИБ.<br>В результате выполнения работы студент получает практические навыки построения составления отчетности внутреннего аудита. |

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 | Информационная безопасность и защита информации : учеб. пособие для студ. вузов по спец. "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - 4-е изд., | URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/10-410.pdf. -Текст : непосредственный.(дата обращения 04.10.2022) |

| | | |
|---|---|---|
| | стер. - М. : Академия, 2009. - 336 с. : ил. - - Библиогр.: с. 327-328. - 2500 экз. - ISBN 978-5-7695-6150-4 (в пер.) : 276.10 р. | |
| 2 | Информационная безопасность персональных компьютеров : учеб. пособие для студ. спец. САПР и строительных спец. по курсу "Методы и средства защиты компьютерной информации". Ч.2 / В.Ю. Смирнов, О.В. Смирнова ; МИИТ. Каф. "САПР транспортных конструкций и сооружений". - М. : МИИТ, 2010. - 88 с. : ил. - Библиогр.: с. 87. - 100 экз. - (в пер.) : 67.66 р. -. | - URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/10-2256.pdf. Текст : непосредственный(дата обращения 04.10.2022) |

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

Антошкин
Станислав
Владимирович

Лист согласования

| | |
|---|---|
| Заведующий кафедрой ВССиИБ | Б.В. Желенков |
| Председатель учебно-методической комиссии | Н.А. Клычева |