МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

30 сентября 2019 г.

Кафедра «Вычислительные системы, сети и информационная безопасность»

Автор Желенков Борис Владимирович, к.т.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Аудит информационной безопасности»

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 2 27 сентября 2019 г. Заведующий кафедрой Б.В. Желенков

Москва 2019 г.

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Аудит информационной безопасности» является формирование компетенций по основам проведения аудита информационной безопасности (ИБ) на предприятии или в организации, изучение видов аудита, необходимых средств и методов для проведения аудита, получение навыков по разработке программы проведения аудита ИБ, выявлению уязвимостей и формированию рекомендаций по устранению уязвимостей.

Основными задачами дисциплины являются:
• ознакомление с целями и задачами проведения аудита информационной безопасности объекта защиты;
• 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 формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной 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
- организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
- поиск рациональных решений при разработке средств защиты информации с учетом

требований качества, надежности и стоимости, а также сроков исполнения;
- осуществление правового, организационного и технического обеспечения защиты информации;

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Аудит информационной безопасности" 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:

ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-9	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПСК-1.4	способность проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей (ПСК-1.4);

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины “Аудит информационной безопасности” осуществляется в форме лекций и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 18 часов, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными).Практические работы организованы с использованием технологий развивающего обучения. Практические работы (26) проводятся в виде упражнений по решению различных вариантов задач аналитического типа или задач разработки с применением интерактивных (диалоговых) технологий в виде мультимедийного лекционного материала (9). Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (58 часов) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям, подготовка к лекциям и практическим работам.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 4 раздела, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков.

Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы. .

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

РАЗДЕЛ 1
Аудит информационной безопасности.

Тема: Основные понятия.
Описываются основные понятия, цели и задачи проведения аудита ИБ. Определяются моменты, когда необходимо проводить аудит, периодичность.

Тема: Виды, этапы и направления деятельности.
Рассматриваются виды и этапы проведения аудита. Описываются направления проведения аудита: первичный аудит; технический аудит, контрольный аудит.

РАЗДЕЛ 2
Нормативно-правовая база проведения аудита ИБ.

Тема: Правовая база проведения аудита.

Тема: Стандарты проведения аудита.
Рассматривается структура международных и национальных стандартов в сфере аудита. Изучаются стандарты ISO 15408 и ISO 17799 и методика их применения для оценки и управления безопасностью информационных технологий.

Тема: Стандарты проведения аудита.
Рассматривается ГОСТ Р ИСО/МЭК 15408, CoBit, PCI DSS. Рассматриваются руководящие документы ФСТЭК России.

Тема: Стандарты проведения аудита.
выполнение лаб.работ 20%

РАЗДЕЛ 3
Методика и порядок проведения аудита ИБ.

Тема: Стадии и методика проведения аудита.
Описываются стадии проведения аудита: планирование, моделирование, тестирование, анализ, разработка предложений, документирование. Рассматриваются экспертно-аналитические, экспертно-инструментальные методы. Анализ бизнес-процессов организации. Моделирование направлений действий злоумышленника.

Тема: Подготовка к аудиту ИБ.
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.

Тема: Планирование аудита.
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.

Тема: Моделирование угроз и тестирование.
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.

Тема: Документирование этапов проведения аудита ИБ.
Рассматриваются рекомендации по документированию: цель и методы обследования, проверка организационно-распорядительных документов, документирование результатов.

РАЗДЕЛ 4
Инструментальные средства проведения аудита ИБ.

Тема: Программное обеспечение для аудита ИБ
Рассматриваются характеристики и обзор программных средств, применяемых для проведения аудита ИБ.

Дифференцированный зачет