

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

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

26 июня 2019 г.


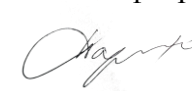
Кафедра «Управление и защита информации»

Автор Сидоренко Валентина Геннадьевна, д.т.н., профессор

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Методы анализа управления рисками»

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>2019</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 25 июня 2019 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 № 21 24 июня 2019 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
--	---

Москва 2019 г.

1. Цели освоения учебной дисциплины

Целями изучения дисциплины «Методы анализа управления рисками» являются теоретическая и практическая подготовка специалистов к деятельности, связанной с управлением рисками, связанными с безопасностью информационных и компьютерных систем.

Задачи дисциплины:

изучение принципов принятия решений в условиях риска и неопределенности;

изучение характеристик полезности;

получение навыков решения задач принятия решений в условиях риска;

получение навыков анализа источников риска и их описания;

получение навыков разработки математических моделей рискованных ситуаций;

получение навыков использования методов решения задач оптимального управления риском.

Основной целью изучения учебной дисциплины «Методы анализа управления рисками» является формирование у обучающегося компетенций для следующих видов деятельности:

эксплуатационная;

специализация №8.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Эксплуатационная деятельность:

проверка технического состояния и профилактические осмотры технических средств защиты информации.

Специализация №8:

разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации, в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Методы анализа управления рисками" 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-1	Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов
ПКР-7	Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации
ПКР-8	Способен подготовить обоснование необходимости защиты информации в автоматизированной системе
ПКР-9	Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой

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 «Методы анализа управления рисками» осуществляется в форме лекций и практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 70 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 30 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция. Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а также использованием компьютерной тестирующей системы. В ходе выполнения курсовой работы реализуются проектные и исследовательские методы обучения. Это позволяет развивать индивидуальные творческие способности обучающихся, более осознанно подходить к профессиональному и социальному самоопределению, самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося. Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относятся отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 5 разделов, представляющих собой логически завершённый объём 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 путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях.

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

РАЗДЕЛ 1

Введение

Предмет курса и его связь со смежными дисциплинами. Библиография. Теория рисков. Риск и неопределенность. Функция полезности. Классификация рисков. Природа рисков. Методы управления рисками в финансовой сфере, банковском деле, страховании. Методы управления рисками в производственной сфере, строительстве. Методы управления рисками в транспортной отрасли, на железнодорожном транспорте, в логистических системах. Методы управления рисками в экологической и социальной сфере, туризме. Проблематика управления информационной безопасностью, анализ средства обеспечения безопасности. Модель безопасности с полным перекрытием. информационной безопасностью, анализ средства обеспечения безопасности. Модель безопасности с полным перекрытием. Программные риски.

РАЗДЕЛ 2

Современные стандарты в области информационной безопасности, использующие концепцию управления рисками

Вопросы стандартизации в области информационной безопасности.

Проблематика управления информационной безопасностью, анализ средства обеспечения безопасности.

ISO/IEC 15408. Критерии оценки безопасности информационных технологий. Стандарты ISO/IEC 17799/27002 и 27001.

ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью".

ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

Системы менеджмента информационной безопасности.

РАЗДЕЛ 3

Методики построения систем защиты информации

Вопросы политики безопасности. Стандарты, процедуры, метрики и анализ рисков.

Методики стратегического планирования построения системы защиты. Модель многоуровневой защиты.

Сбор данных об информационной системе с помощью средств администрирования.

Сбор данных о топологии сети с помощью средства администрирования сетей.

Использование сканеров безопасности для получения информации о сети.

Выявление уязвимостей.

РАЗДЕЛ 4

Методики и программные продукты для оценки рисков

Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методика Microsoft. Анализ существующих подходов.

РАЗДЕЛ 5

Методы совершенствования системы управления информационной безопасностью компьютерной системы

Локальная политика паролей. Управление разрешениями на файлы и папки.

Использование цифровых сертификатов. Центр сертификации (удостоверяющего центра) в ОС Unix и Microsoft.

Идентификация и аутентификация. Протокол Kerberos.

Шифрование данных при хранении.

Межсетевые экраны Встроенный межсетевой экран (firewall). Настройка протокола IPSec.

Автоматическое обновление операционной системы с использованием службы WSUS.
Установка сервера обновлений. Управление обновлениями. Распространение обновлений.

РАЗДЕЛ 6
Зачет с оценкой