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 Сафонова Ирина Евгеньевна, д.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Методы оценки безопасности компьютерных систем

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/а 27 сентября 2019 г. Заведующий кафедрой  Б.В. Желенков

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Методы оценки безопасности компьютерных систем» являются формирование компетенций по основным разделам данного курса, изучение студентами основных методов оценки безопасности компьютерных систем, стандартов в этой области; получение представления об организации и принципах обеспечения информационной безопасности компьютерных систем.
Студенты должны научиться применять современные методы оценки безопасности компьютерных систем.
Основными задачами дисциплины являются:
- Ознакомление с оценочными стандартами и техническими спецификациями.
- Изучение методов оценки безопасности компьютерных систем.
- Изучение формальных и неформальных средств защиты.
- Изучение стандартов информационной безопасности.

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:
- 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. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Методы оценки безопасности компьютерных систем" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Криптографические методы защиты информации:

Знания: понятия, определения, термины (понятийный аппарат курса)принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах

Умения: оформлять, представлять, описывать, характеризовать данные, сведения, факты, результаты работы на языке символов (терминов, формул, образов), введенных и используемых в курсеиспользовать основные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельностиформировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностьюучаствовать в работах по реализации политики информационной безопасности

Навыки: проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности

2.1.2. Основы информационной безопасности :

Знания: принципы и методы организационной защиты информацииправовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайныпринципы организационной защиты информации методологические и технологические основы комплексного обеспечения безопасности компьютерных систем, угрозы и методы нарушения безопасности, формальные модели по оценке защищенностиматематические основы криптографии, технические и программные средства защиты информации в современных компьютерных системах и сетях, методы шифрования информацииипринципы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации

Умения: анализировать и оценивать угрозы информационной безопасности объектаприменять известные методы и средства поддержки информационной безопасности в компьютерных системахосуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защитыопределять рациональные способы и средства защиты информации на объекте информатизации с учетом затрат на них

Навыки: безопасного использования технических средств в профессиональной деятельности средствами выявления угроз безопасности для компьютерных систем

2.2. Наименование последующих дисциплин

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПСК-1.2 способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПСК 1.2);	Знать и понимать: состав и назначение компонентов системы защиты информации; объяснять взаимосвязь объектов в информационной системе. Уметь: сопоставлять степень угрозы информационной безопасности и стоимость соответствующих средств защиты. Владеть: основными приемами оценки и анализа эффективности использования средств обеспечения информационной безопасности.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

3 зачетные единицы (108 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 7
Контактная работа	32	32,15
Аудиторные занятия (всего):	32	32
В том числе:		
лекции (Л)	14	14
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	40	40
Экзамен (при наличии)	36	36
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

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

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	7	Раздел 1 Обеспечение информационной безопасности.	2		4/2		8	14/2	
2	7	Тема 1.5 Стандарты безопасности в сети Internet.	2					2	ПК1, (контрольная работа №1)
3	7	Раздел 2 Критерии безопасности компьютерных систем CTCPEC. Рекомендации X.800 для распределенных систем.	4		4/2		8	16/2	
4	7	Тема 2.4 Критерии аудита (регистрация и учет событий в системе; идентификация и аутентификация).	4					4	
5	7	Раздел 3 Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга).	4		2/2		8	14/2	
6	7	Тема 3.1 Основные группы безопасности (группа D - Minimal Protection (минимальная защита); группа C - Discretionary Protection (избирательная защита); группа B - Mandatory Protection (полномочная защита) группа A - Verified Protection (проверяемая защита)).	2					2	
7	7	Тема 3.2 Классы безопасности (класс C1 -	2					2	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Discretionary Security Protection (избирательная защита безопасности) ; класс C2 - Controlled Access Protection (защита контролируемого доступа),класс B1 - Labeled Security Protection (меточная защита безопасности); класс B3 - Security Domains (области безопасности); класс A1 - Verified Desing (проверяемая разработка))							
8	7	Раздел 4 Гармонизированные критерии оценки безопасности информационных технологий ITSEC.	2		4/2		8	14/2	
9	7	Тема 4.3 Сетевые конфигурации (требования к обеспечению конфиденциальности и целостности информации в сетевых конфигурациях).	2					2	ПК2, (контрольная работа №2)
10	7	Раздел 5 Общие критерии оценки безопасности информационных технологий.	2		4/1		8	14/1	
11	7	Тема 5.4 Критерии оценки для профилей защиты.	2					2	
12	7	Раздел 7 Итоговая аттестация						36	ЭК
13		Тема 1.1 Формальные методы доказательства правильности программ и их спецификаций							
14		Тема 1.2							

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Методы и средства анализа безопасности программного обеспечения (контрольно-испытательные методы логико-аналитические методы).							
15		Тема 1.3 Федеральные критерии безопасности информационных технологий.							
16		Тема 1.4 Защита АС и средств СВТ.							
17		Тема 2.1 Функциональные критерии. Критерии конфиденциальности (контроль скрытых каналов; произвольное управление доступом; нормативное управление доступом; повторное использование объектов).							
18		Тема 2.2 Критерии целостности (домены целостности; произвольное управление целостностью; нормативное управление целостностью; физическая целостность; возможность осуществления отката; разделение ролей; самотестирование).							
19		Тема 2.3 Критерии работоспособности							

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		(контроль за распределением ресурсов; устойчивость к отказам и сбоям; живучесть; восстановление).							
20		Тема 4.1 Гарантированность безопасности (семь возможных уровней гарантированности корректности - от E0 до E6; общая оценка системы).							
21		Тема 4.2 Требования к политике безопасности (требования к наличию защитных механизмов; дополнительные классы).							
22		Тема 5.1 Классификация набора требований безопасности (общие положения, структуры группирования и принципы целевого использования требований безопасности).							
23		Тема 5.2 Объект оценки (понятие, представление и общая модель).							
24		Тема 5.3 Требования безопасности (требования к функциям безопасности, требования гарантии безопасности).							
25		Всего:	14		18/9		40	108/9	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	7	РАЗДЕЛ 1 Обеспечение информационной безопасности.	Оценка технологической безопасности программного продукта.	4 / 2
2	7	РАЗДЕЛ 2 Критерии безопасности компьютерных систем CTCPEC. Рекомендации X.800 для распределенных систем.	Оценка безопасности информационной системы по критериям CTCPEC.	4 / 2
3	7	РАЗДЕЛ 3 Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга).	Оценка безопасности информационной системы по критериям TCSEC.	2 / 2
4	7	РАЗДЕЛ 4 Гармонизированные критерии оценки безопасности информационных технологий ITSEC.	Оценка безопасности информационной системы по критериям ITSEC.	4 / 2
5	7	РАЗДЕЛ 5 Общие критерии оценки безопасности информационных технологий.	Оценка безопасности информационной системы по общим критериям.	4 / 1
			ВСЕГО:	18/9

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) учебным планом не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Методы оценки безопасности компьютерных систем» осуществляется в форме лекций и практических занятий.
Лекции проводятся в традиционной классно-урочной организационной форме в объеме 18 часов, по типу управления познавательной деятельностью на 100% являются традиционными классически-лекционными (объяснительно-иллюстративными).
Практические работы (36 часов) организованы с использованием технологий развивающего обучения, проводится с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники); технологий, основанных на коллективных способах обучения.
Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (49 часов) относится отработка лекционного материала.
Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 5 разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают вопросы теоретического характера для оценки знаний. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	7	РАЗДЕЛ 1 Обеспечение информационной безопасности.	1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №1. 3. Изучение учебной литературы из приведенных источников: [1, стр.50-74, [3, стр. 50-74], 1 [10-17].	8
2	7	РАЗДЕЛ 2 Критерии безопасности компьютерных систем CTCPEC. Рекомендации X.800 для распределенных систем.	1. Анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №2. 3. Изучение учебной литературы из приведенных источников: 1 [1, стр. 70-94], [2, стр.22-41].	8
3	7	РАЗДЕЛ 3 Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга).	1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №3. 3. Изучение учебной литературы из приведенных источников: [3, стр. 45-61].	8
4	7	РАЗДЕЛ 4 Гармонизированные критерии оценки безопасности информационных технологий ITSEC.	1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №4. 3. Изучение учебной литературы из приведенных источников: [1, стр.40-58], [2, стр.38-40, 44-61] [3, стр.45-61].	8
5	7	РАЗДЕЛ 5 Общие критерии оценки безопасности информационных технологий.	1. Дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №5. 3. Изучение учебной литературы из приведенных источников: [1, стр. 221-235], [3, стр.45-61], [4, стр.98-130].	8
			ВСЕГО:	40

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Информационная безопасность и защита информации	В.П. Мельников, С.А. Клейменов, А.М. Петраков	МИИТ НТБ, 2012	Все разделы
2	Безопасность коммуникационных сетей	В.П. Соловьев, А.Е. Шубарев, Н.Н. Пуцко	МИИТ НТБ, 2007	Все разделы
3	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства)	А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров	МИИТ НТБ, 2006	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Технические, организационные и кадровые аспекты управления информационной безопасностью.	Милославская Н., Сенаторов М., Толстой А.	М.:Горячая линия , 2014	Все разделы

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

• Форум специалистов по информационным технологиям http://citforum.ru/
• Интернет-университет информационных технологий http://www.intuit.ru/
• Электронный фонд правовой и нормативно-технической документацииhttp://docs.cntd.ru/
• ГОСТ РФ http://gostrf.com/
• http://dehack.ru
• www.securitylab.ru

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Microsoft Windows
Microsoft Office
Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014
Microsoft Windows
Microsoft Office
Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

Putty
Бесплатноеиспользование (MIT)

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций
№1329
Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.
Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ
№1327
Рабочие станции для студентов 17шт, коммутатор CISCO – 9шт, маршрутизатор CISCO – 9шт, сетевое оборудование, рабочая станция преподавателя, проектор, экран, доска

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Студентам необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Студент должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.
Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.
Главная задача лекционного курса – сформировать у студентов системное представление об изучаемом предмете, обеспечить усвоение основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.
Основные функции лекций:
- познавательно-обучающая;
- развивающая;
- ориентирующе-направляющая;
- активизирующая;
- воспитательная;
- организующая;
- информационная.

Выполнение практических занятий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств бакалавров.Практическиезанятия(22 часа, в том числе 6 часов в интерактивной форме) организованы с использованием технологий развивающего обучения,проводится с использованием интерактивных (диалоговых) технологий.
Проведение практических занятий не сводится только к органичному дополнению лекционных курсов и самостоятельной работы студентов. Практические занятия следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы.
Задачи практических занятий – закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной

литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Каждому студенту следует составлять еженедельный семестровый план работы, а также план на каждый учебный день. Нужно осуществлять самоконтроль, который является необходимым условием успешной работы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к зачету и контрольные работы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Фонд оценочных средств является составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины.

Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.