МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Методы оценки защищенности компьютерных систем

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой  Л.А. Баранов

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями изучения дисциплины «Методы оценки защищенности компьютерных систем» являются овладение студентами теоретических и практических основ организации и проведения оценки безопасности компьютерных систем; развитие в процессе обучения системного мышления, необходимого для решения задач программной защиты информации с учетом требований системного подхода; обучение студентов принципам построения защиты информации в ОС и анализа надежности, защиты компьютерных системах.

Задачи дисциплины:

изучение принципов построения подсистем защиты в компьютерных системах различной архитектуры;

изучение средств и методов несанкционированного доступа к ресурсам компьютерных систем;

изучение системного подхода к проблеме защиты информации в компьютерных системах;

изучение механизмов защиты информации и возможностей по их преодолению.

Основной целью изучения учебной дисциплины «Методы оценки защищенности компьютерных систем» является формирование у обучающегося компетенций для следующих видов деятельности:

научно-исследовательская;

организационно-управленческая.

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

Научно-исследовательская деятельность:

сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;

изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;

подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

Организационно-управленческая деятельность:

организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

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

2.1. Наименования предшествующих дисциплин

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	ПКР-1 Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	ПКР-1.1 Строит математические модели для оценки безопасности компьютерных систем. ПКР-1.2 Анализирует компоненты системы безопасности с использованием современных математических методов.
2	ПКР-10 Способен проводить тестирование систем защиты информации автоматизированных систем	ПКР-10.1 Проводит индивидуальное тестирование систем защиты информации в блоке автоматизированных систем.
3	ПКР-7 Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	ПКР-7.1 Разрабатывает математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации. ПКР-7.2 Анализирует математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации. ПКР-7.3 Обосновывает адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
4	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-2.1 Знать основные процессы проектирования систем обеспечения информационной безопасности. ПКС-2.2 Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.
5	ПКС-4 Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем	ПКС-4.1 Знать основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении. ПКС-4.2 Уметь создавать системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации. ПКС-4.3 Владеть навыками создания систем обеспечения информационной безопасности.
6	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	ПКС-5.1 Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации. ПКС-5.2 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. ПКС-5.3 Владеть навыками разработки нормативной правовой документации.

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

4.1. Общая трудоемкость дисциплины составляет:

4 зачетные единицы (144 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 10
Контактная работа	54	54,15
Аудиторные занятия (всего):	54	54
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	54	54
Экзамен (при наличии)	36	36
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	10	Раздел 1 Введение Предметная область оценки защищенности компьютерных систем. История развития защиты информации и криптографии.	2		2		10	14	
2	10	Раздел 2 Методы и средства оценки защищённости компьютерных систем Конкурентная разведка. Поиск информации в открытых источниках. Основные виды уязвимостей.	14		8		22	44	ПК1
3	10	Раздел 3 Инструментарий для оценки защищённости компьютерных систем Освоение сканнеров уязвимостей, фаззеров. Освоение анализаторов кода, инструментов изучения сети. Освоение специализированных дистрибутивов.	20		8		22	50	ПК2
4	10	Экзамен						36	ЭК
5		Всего:	36		18		54	144	

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	10		Введение Предметная область оценки защищенности компьютерных систем. История развития защиты информации и криптографии.	2
2	10		Методы и средства оценки защищённости компьютерных систем Конкурентная разведка. Поиск информации в открытых источниках. Основные виды уязвимостей.	8
3	10		Инструментарий для оценки защищённости компьютерных систем Освоение сканнеров уязвимостей, фаззеров. Освоение анализаторов кода, инструментов изучения сети. Освоение специализированных дистрибутивов.	8
			ВСЕГО:	18 / 0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Методы оценки защищенности компьютерных систем» осуществляется в форме лекций, лабораторных работ и практических занятий.
Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция.
Практические занятия и лабораторные работы организованы с использованием технологий развивающего обучения.
В ходе выполнения лабораторных работ 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 относиться 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 6 разделов, представляющих собой логически завершенный 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.

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	10		Введение Предметная область оценки защищенности компьютерных систем. История развития защиты информации и криптографии.	10
2	10		Методы и средства оценки защищённости компьютерных систем Конкурентная разведка. Поиск информации в открытых источниках. Основные виды уязвимостей.	22
3	10		Инструментарий для оценки защищённости компьютерных систем Освоение сканнеров уязвимостей, фаззеров. Освоение анализаторов кода, инструментов изучения сети. Освоение специализированных дистрибутивов.	22
			ВСЕГО:	54

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. Словарь по терминологии	Гончаров И.В., Кирсанов Ю.Г., Райков О.В.	ЗАО«НПО Инфобезопасность», 2015 ЭБС	Все разделы
2	Информационная безопасность и защита информации	В.П. Мельников, С.А. Клейменов, А.М. Петраков	Издательский центр "Академия", 2012 ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)	Все разделы
3	Защита информации: учеб. пособие	И.К. Астанин, Н.И. Астанин	Воронеж. Гос. Ун-т, 2006 ЭБС	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	"Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие.	Андрианов В.И., Бородин В.А., Соколов А.В.	Лань, 1996 ЭБС	Все разделы
5	Методы и инженерно–технические средства противодействия информационным угрозам	Абалмазов Э.И.	Маршрут, 2005 ЭБС	Все разделы

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

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ.
http://elibrary.ru/ - научно-электронная библиотека.
www.chipinfo.ru
http://siblec.ru/
www.defcon.ru
http://xakep.ru/
http://kali.org/
http://www.intuit.ru
http://habrahabr.ru
http://semestr.ru
http://www.intersystems.ru
Поисковые системы: Yandex, Google, Mail.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ,

ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
Для проведения практических занятий необходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами:
Microsoft Office не ниже Microsoft Office 2007 (2013),
программа виртуализации ОС VirtualBox,
платформа для проведения аудита безопасности веб-приложений Burp Suite
программа-анализатора трафика для компьютерных сетей Wireshark
специализированный дистрибутив Kali Linux / windows-платформа для тестов на проникновение PentestBox
среда визуального программирования MicroSoft Visual Studio 2013.

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

Для проведения аудиторных занятий и самостоятельной работы требуется:
1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET.
2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET
4. Для проведения практических занятий: компьютерный класс; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

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

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе.
Обучающийся 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 обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.
Основные функции лекций: 1. Познавательно-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. информационная.
Выполнение практических заданий и лабораторных работ 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 будущих специалистов.
Проведение практических занятий и лабораторных работ не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.
При подготовке специалиста важна не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий и лабораторных работ. Задачи практических занятий и лабораторных работ: 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 и лабораторной работе 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 и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. 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 экзамену и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.
Фонд оценочных средств являются 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.