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)

Методы оценки безопасности компьютерных систем

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 17.02.2024

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Методы оценки безопасности компьютерных систем» является формирование профессиональных компетенций по основным разделам дисциплины.

Основными задачами дисциплины являются:

- изучение 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 на практике.

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;

ОПК-11 - Способен проводить эксперименты по заданной методике и обработку их результатов ;

ПК-5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ;

ПК-11 - способностью принимать участие в проведении экспериментальных исследований системы защиты информации.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

виды политик управления доступом и информационными потоками в компьютерных сетях и системах; методы оценки безопасности компьютерных систем.

Уметь:

обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях и системах; использовать на практике методы оценки безопасности компьютерных систем.

Владеть:

навыками разработки порядка применения программно-аппаратных средств защиты информации в компьютерных системах и сетях.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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. №7
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

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 96 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. ВВЕДЕНИЕ В ДИСЦИПЛИНУ. Рассматриваемые вопросы: - обеспечение безопасности компьютерных систем; - основные понятия, виды; - требования к политике безопасности; - классификация методов оценки безопасности КС. 2. БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Рассматриваемые вопросы: - формальные методы доказательства правильности программ и их спецификаций; - методы и средства анализа безопасности программного обеспечения: контрольно-испытательные методы логико-аналитические методы. 3. БЕЗОПАСНОСТЬ ТЕХНИЧЕСКИХ СРЕДСТВ КОМПЬЮТЕРНЫХ СИСТЕМ. Рассматриваемые вопросы: - основные определения; - анализ безопасности технических средств компьютерных систем; - подходы к организации и к оценке информационной безопасности. 4. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ. Рассматриваемые вопросы: - рекомендации X.800, общие критерии оценки безопасности информационных технологий, ISO/IEC 27000:2018 и другие; - функции и механизмы безопасности, администрирование средств безопасности, набор требований безопасности. - объект оценки; - критерии оценки для профилей защиты; - сетевые конфигурации (требования к обеспечению конфиденциальности и целостности информации в сетевых конфигурациях). 5. НАЦИОНАЛЬНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ. Рассматриваемые вопросы: - обзор стандартов; - критерии оценки пригодности компьютерных систем TCSEC; - критерии безопасности компьютерных систем CTCPEC; - гармонизированные критерии оценки безопасности информационных технологий ITSEC; - канадские критерии; - ГОСТы. 6. ФЕДЕРАЛЬНЫЕ СТАНДАРТЫ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. Рассматриваемые вопросы: - критерии, ГОСТы, руководящие и нормативные документы; - защита автоматизированных систем и средств вычислительной техники: классификация, требования по защите информации от НСД, классы защищенности. - стандарты безопасности в сети Internet: МЭ, протоколы защищенной передачи информации. 7. СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ. Рассматриваемые вопросы: - понятие систем управления информационной безопасностью, функции; - выявление и анализ рисков информационной безопасности (ИБ);

№ п/п	Тематика лекционных занятий / краткое содержание
	- планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ, контролирование этих процессов; - внесение в процессы минимизации информационных рисков необходимых корректировок. 8. КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКИ БЕЗОПАСНОСТИ КС. Рассматриваемые вопросы: - качественное управление информационной безопасностью; - рискообразующие факторы, уровень управляемости, адекватность используемой и генерируемой информации; - эффективность СУИБ как баланс между возможностями, производительностью и издержками; - непрерывность управления, процессный подход.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	1 ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Результат работы – список угроз и мер по разработке безопасного ПО, согласно ГОСТ Р 58412-2019. 2 МЕЖСЕТЕВЫЕ ЭКРАНЫ. Результат работы – анализ профилей защиты МЭ. 3 ОБЩИЕ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. Результат работы – навыки практического применения соответствующего стандарта. 4 РЕКОМЕНДАЦИИ X.800 ДЛЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ. Результат работы – навыки практического применения соответствующего стандарта. 5 ЗАЩИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. Результат работы – навыки практического применения Руководящего документа. 6 ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ. Результат работы – навыки практического применения Руководящего документа. 7 БЕЗОПАСНОСТЬ КОМПЬЮТЕРНОЙ СЕТИ. Результат работы – схема компьютерной сети, в которой защищены административный доступ к устройствам и трафик протоколов маршрутизации. 8 ОЦЕНКА БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СИСТЕМЫ Результат работы – оценка безопасности и список рекомендаций по повышению безопасности КС

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом. Подготовка к практическим занятиям.

2	Подготовка к промежуточной аттестации.
3	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с.	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (дата обращения: 16.02.2024). - Текст:
2	Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения. М.: Юрайт. 2021. - 312с.ISBN 978-5-534-13221-2.	https://book-pc.ru/bezopasnost/1882-programmno-apparatnye-sredstva-zaschity-informacii.html (дата обращения: 16.02.2024). - Текст: электронный
3	Паршин К.А. Оценка уровня информационной безопасности на объекте информатизации: учебное пособие для студ. вузов ж.-д. трансп. М.: ФГБОУ "УМЦ ЖДТ". 2015. - 95 с.	https://umczdt.ru/books/1094/30046/(дата обращения:16.02.2024).- Текст: электронный.
4	Деза Е., Котова Л. Введение в криптографию: Теоретико-числовые основы защиты информации. Ленан. 2021. – 376с.	https://book-pc.ru/bezopasnost/1727-vvedenie-v-kriptografiju.html(дата обращения:16.02.2024).- Текст: электронный.

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Поисковые системы: Yandex, Google, Mail.

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Специализированное программное обеспечение не требуется.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения аудиторных занятий и самостоятельной работы требуются:

Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET

Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения практических занятий:

компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB.

9. Форма промежуточной аттестации:

Экзамен в 7 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

профессор, доцент, д.н. кафедры «Вычислительные системы, сети и информационная безопасность» И.Е. Сафонова

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической комиссии Н.А. Андриянова