МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмшин

10.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МЕТОДЫ И СТАНДАРТЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	8

Магнитогорск
2023 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
09.02.2023, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
10.02.2023 г. протокол № 7

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
Зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО), _____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целями изучения дисциплины «Методы и стандарты оценки защищенности компьютерных систем» является формирование у обучающихся понятий о принципах и методах оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности; критериях оценки безопасности информационных технологий; отечественных и международных стандартах оценки защищенности информационных систем; освоение методов качественной и количественных оценок систем информационной безопасности в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Методы и стандарты оценки защищенности компьютерных систем входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Информатика

Сети и системы передачи информации

Безопасность систем баз данных

Безопасность сетей ЭВМ

Безопасность операционных систем

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Анализ рисков информационной безопасности

Защита информационно-технологических ресурсов автоматизированных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

Подготовка к сдаче и сдача государственного экзамена

Производственная - научно-исследовательская работа

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Методы и стандарты оценки защищенности компьютерных систем» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-1 Способен проводить анализ безопасности компьютерных систем	
ПК-1.1	Оценивает эффективность защиты информации
ПК-1.2	Применяет разработанные методики оценки защищенности программно-аппаратных средств защиты информации

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:
– контактная работа – 72 акад. часов:
– аудиторная – 68 акад. часов;
– внеаудиторная – 4 акад. часов;
– самостоятельная работа – 36,3 акад. часов;
– в форме практической подготовки – 0 акад. час;
– подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Общие вопросы оценки безопасности компьютерных систем								
1.1 Стандарт "Критерии определения безопасности компьютерных систем"/ "Оранжевая книга".	8	1		1	1,5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-1.1, ПК-1.2

1.2 Стандарт ISO/IEC 15408 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.		1		1	1,5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-1.1, ПК-1.2
1.3 ISO 17799 Практические правила менеджмента информационной безопасности		1		1	1,5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-1.1, ПК-1.2
1.4 Российские стандарты и руководящие документы в области оценки защищенности		1		1	0,5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-1.1, ПК-1.2
Итого по разделу		4		4	5			
2. Методы оценки систем информационной								

2.1 Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников. Построение графа атак	8	4		4	3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование, Практическая работа 1	ПК-1.1, ПК-1.2
2.2 Тестирование систем информационной безопасности		6		4	3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование	ПК-1.1, ПК-1.2
2.3 Метод экспертных оценок		4		4	3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование. АКР 1	ПК-1.1, ПК-1.2

2.4 Метод информационных потоков .		4		4	2,3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование. АКР 2	ПК-1.1, ПК-1.2
2.5 Оценка показателей защиты информации с применением диаграммы Парето		6		6	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование. АКР 3	ПК-1.1, ПК-1.2
2.6 Метод весовых коэффициентов		4		4	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование. АКР 4	ПК-1.1, ПК-1.2
Итого по разделу		28		26	15,3			
3. Организация оценки безопасности компьютерных систем								

3.1 Формирование экспертных систем оценки безопасности компьютерных систем	8	2		4	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Компьютерное тестирование, Практическая работа 2	ПК-1.1, ПК-1.2
Итого по разделу		2		4	4			
4. Экзамен								
4.1 Экзамен	8				12	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);	Экзамен	ПК-1.1, ПК-1.2
Итого по разделу					12			
Итого за семестр		34		34	36,3		экзамен	
Итого по дисциплине		34		34	36,3		экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Методы и стандарты оценки защищенности компьютерных систем» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций , учета особенностей профессиональной деятельности выпускников и потребностей работодателей

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1.Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772

2. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901

б) Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 31.01.2023).

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 31.01.2023)

МАКРООБЪЕКТЫ:

3. Баранкова И. И. Сетевая защита информации. Лабораторный практикум [Электронный ресурс] : учебное пособие [для вузов] / И. И., Баранкова, Д.Н. Мазнин, У.В. Михайлова, М.В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - ISBN 978-5-9967-1605-0 URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения 31.01.2023)

4. Баранков В. В. Развертывание и настройка виртуальных сетей [Электронный ресурс] : учебное пособие [для вузов] / В. В. Баранков, И. И. Баранкова, У. В.

Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - ISBN 978-5-9967-1305-9 URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3813.pdf&show=dcatalogues/1/1529986/3813.pdf&view=true (дата обращения 31.01.2023)

5. Архитектура и принципы работы вычислительных систем [Электронный ресурс] : учебное пособие [для вузов] / В.В. Баранков, И.И. Баранкова, М.В. Афанасьева, М.В. Коновалов; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - ISBN 978-5-9967-1306-6 URL : https://magtu.informsystema.ru/uploader/fileUpload?name=3924.pdf&show=dcatalogues/1/1530495/3924.pdf&view=true (дата обращения 31.01.2023)

6. Баранкова, И. И. Михайлова У.В. , Лукьянов Г.И. Техническая защита информации. Лабораторный практикум [Электронный ресурс] : учебное пособие / МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). URL : https://magtu.informsystema.ru/uploader/fileUpload?name=2935.pdf&show=dcatalogues/1/1134667/2935.pdf&view=true (дата обращения 31.01.2023)

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта

*При открытии макрообъектов учитывайте настройки антивирусной защиты

в) Методические указания:

1. Методические указания по выполнению практических работ по дисциплине «Методы и стандарты оценки защищенности компьютерных систем» (Приложение 1) .

2. Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Методы и стандарты оценки защищенности компьютерных систем» (Приложение 2).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
Oracle Virtual Box	свободно распространяемое ПО	бессрочно
MS SQL Server Management Studio	свободно распространяемое ПО	бессрочно
Oracle My SQL Workbench Community Edition	свободно распространяемое ПО	бессрочно
Oracle SQL Developer	свободно распространяемое ПО	бессрочно

LibreOffice	свободно	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
MS Visual Studio 2017 Community	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер	свободно	бессрочно
MariaDB	свободно	бессрочно
PostgreSQL	свободно	бессрочно
MS Office 2003	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно	бессрочно
Linux	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services,	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://magtu.informsystema.ru/Marc.html?locale=ru
Федеральный образовательный портал – Экономика. Социология.	http://ecsocman.hse.ru/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer	https://www.nature.com/siteindex
Архив научных журналов «Национальный электронно-информационный	https://archive.neicon.ru/xmlui/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и	https://fstec.ru/dokumenty-filter

Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)- Мультимедийные средства хранения, передачи и представления информации

Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.) - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Аудитория для самостоятельной работы читальные залы библиотеки, ауд 132а - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Методы и стандарты оценки защищенности компьютерных систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания и вопросы по темам:

Перечень вопросов контрольных работ и тестирования по темам разделов 1-4:

1. Что такое классы безопасности и уровни доверия?
2. Дайте понятие сетевой доверенной вычислительной базы.
3. Какие существуют сервисы безопасности?
4. Какие существуют механизмы реализации сервисов безопасности?
5. Какие выделяют этапы жизненного цикла объекта оценки?
6. Перечислите классы функциональных требований в ISO 15408.
7. Перечислите классы требований доверия в ISO 15408.
8. Перечислите оценочные уровни доверия в стандарте ISO 15408.
9. Перечислите группы элементов управления в стандарте ISO 17799.
10. Перечислите ключевые элементы управления в ISO 17799.
11. Что включает в себя типовая методика анализа защищенности ИС
12. предприятия?
13. Какие исходные данные необходимы для анализа защищенности ОИ?
14. Какова цель тестирования системы защиты?
15. Что из себя представляет тестирование по методу "черного ящика"?
16. Что из себя представляет тестирование по методу "белого ящика"?
17. Что из себя представляет тест на проникновение?
18. На чем основан метод экспертных оценок?
19. Как определить риски через коэффициенты значимости?
20. Какие варианты информационных потоков могут быть между отправителем и получателем?
21. Как строится алгоритм распределения функций безопасности?
22. Каким образом определяется факт защищенности?
23. От чего зависит оценочный параметр защищенности?
24. Какие выводы можно сделать, если параметр защищенности
25. меньше 1, больше 1 и много больше 1?

Пример АКР 2. Метод информационных потоков

Сеть(рис.1) включает в себя две доверенных между собой локальных сети, связанных через Интернет. Первая локальная сеть включает в себя: FIREWALL – межсетевой фильтр, DOM1 – сервер (контроллер домена), SMTP1 – почтовый сервер и состоит из двух сегментов. К первому сегменту относятся ПК PC11,…,PC1n, а во второй сегмент входят рабочие станции PC21,…,PC2m. Пусть вторая локальная сеть состоит из FIREWALL – межсетевого фильтра, DOM2 – сервера, SMTP2 – почтового сервера, рабочих станций PC31,…,PC3k. Будем считать, что каждый компьютер является персональным, т.е. на нем работает и обладает правами доступа только один конкретный пользователь.

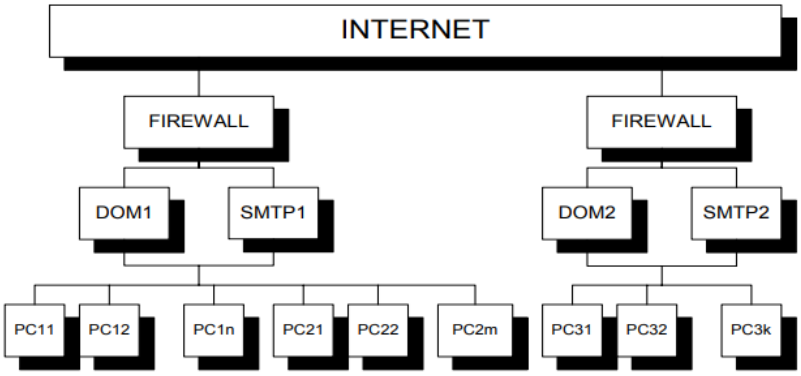

Рис.1 – Примерная топология сети

Определить всевозможные информационные потоки. Составить матрицу разрешенных связей. Определить возможность атак (например: Атака протокола TCP).

Приложение 2

7Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-1 Способен проводить анализ безопасности компьютерных систем		
ПК-1.1	Оценивает эффективность защиты информации	Перечень вопросов: 1. Что такое уровень гарантированности? 2. Какие виды гарантированности бывают? 3. Что такое классы безопасности и уровни доверия? 4. Перечислите классы функциональных требований в ISO 15408. 5. Перечислите классы требований доверия в ISO 15408. 6. Перечислите оценочные уровни доверия в стандарте ISO 15408. 7. Перечислите группы элементов управления в стандарте ISO 17799. 8. Перечислите ключевые элементы управления в ISO 17799. 9. Средства защиты в компьютерных системах 10. Теоретико-вероятностный метод оценки защищенности в компьютерных системах 11. Экспертный метод оценки в компьютерных системах 12. Статистический метод оценки в компьютерных системах 13. Вероятностно-статистический метод оценки рисков в компьютерных системах 14. Взаимосвязь угроз, уязвимостей и рисков 15. Оценки защищенности на основе модели комплекса механизмов защиты 16. Семантические показатели защищенности компьютерных систем 17. Нечеткие оценки защищенности компьютерных систем 18. Комплексные оценки защищенности компьютерных систем 19. Типовая архитектура системы выявления атак Методы тестирования системы защиты
ПК-1.2	Применяет разработанные методики оценки защищенности программно-аппаратных средств защиты	Задание: Оценить показатели защиты информации для заданной системы Виды систем:

	информации	1. Информационно-поисковые системы 2. Электронный документооборот и делопроизводство 3. Электронные архивы 4. Системы управления ресурсами организации 5. Системы автоматизации проектирования 6. Информационно-аналитические системы 7. Системы поддержки принятия решений 8. Системы видеоконференцсвязи и цифровой телефонии 9. Ситуационные и управляющие центры Построить причинно-следственную диаграмму Исикавы для выявления и ранжирования имеющихся причинно-следственных связей возникновения угроз Используя метод оценки защищенности на основе модели комплекса механизмов защиты определить защищенность, обеспечиваемой отдельным механизмом и СЗИ в целом. Определить эффективность применяемых методов обеспечения безопасности компьютерной системы. Используя онлайн-калькулятор банка данных угроз ФСТЭК определить базовые, временные и контекстные метрики угроз информационной безопасности компьютерных систем

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Критерии оценки (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

ПРИЛОЖЕНИЕ 3

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

Рекомендации направлены на оказание методической помощи обучающимся при выполнении практических занятий.

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение практических навыков решения типовых и прикладных задач.

Целью практических занятий является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;
- приобретение обучающимися умений и навыков использования современных теоретических знаний в решении конкретных практических задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем практических занятий определяется рабочей программой дисциплины. План практических занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности обучающихся к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ обучающиеся допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения практических работ

При подготовке к выполнению практических работ обучающийся должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым обучающимся самостоятельно, согласно индивидуальному заданию.

Обучающиеся, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы обучающийся демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если обучающийся набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя, или работа не выполнена.