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

26.01.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕСТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация №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	5
Семестр	10

Магнитогорск
2022 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
25.01.2022, протокол № 4

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.01.2022 г. протокол № 5

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 2022 - 2023 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 2023 - 2024 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 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

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Тестирование систем защиты информации автоматизированных систем» является формирование у обучающихся понятий о принципах построения и функционирования систем и сетей передачи информации; основных угрозах безопасности информации и модели нарушителя в автоматизированных системах; основных мерах по защите информации в автоматизированных системах; принципах построения средств защиты информации от утечки по техническим каналам; составления методик тестирования систем защиты информации автоматизированных систем; подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; составление протоколов тестирования систем защиты информации автоматизированных систем и новейшие технические; программных средствах контроля эффективности мер защиты информации; нормативных правовых актах в области защиты информации; руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Тестирование систем защиты информации автоматизированных 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

Сети и системы передачи информации

Программно-аппаратные средства обеспечения информационной безопасности

Безопасность систем баз данных

Безопасность сетей ЭВМ

Разработка систем защиты информации автоматизированных систем

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

Обеспечение информационной безопасности критической информационной инфраструктурой

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Форензика

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

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

В результате освоения дисциплины (модуля) «Тестирование систем защиты информации автоматизированных систем» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	
ПК-6.1	Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью

	выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем
ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах
ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 103,8 акад. часов:

– аудиторная – 102 акад. часов;

– внеаудиторная – 1,8 акад. часов;

– самостоятельная работа – 40,2 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет

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. Сертификация средств защиты информации автоматизированных систем								
1.1 Общие сведения. Организационная структура системы сертификации. Подача заявки на сертификацию.	10	4	10/4И		6	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4
1.2 Принятие решения о проведении сертификации средства защиты информации. Сертификационные испытания средства защиты информации.		6	10/2И		4	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4

1.3 Оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия. Маркирование средств защиты информации. Внесение изменений в сертифицированное средство защиты информации. Переоформление, продление, приостановление и прекращение сертификата		6	12/5И		6	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4
Итого по разделу		16	32/11И		16			
2. Аттестации автоматизированных систем с учетом нормативных документов по защите информации								
2.1 Общие положения. Организационная структура системы аттестации.	10	4	10/2И		6	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4
2.2 Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте. Порядок проведения аттестации и контроля		6	12/4,8И		8	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4

2.3 Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации.		8	14/6И		10,2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4
Итого по разделу		18	36/12,8И		24,2			
Итого за семестр		34	68/23,8И		40,2		зачёт	
Итого по дисциплине		34	68/23,8 И		40,2		зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Тестирование систем защиты информации автоматизированных 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(дата обращения: 31.08.2020).

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/441287 (дата обращения: 31.08.2020).

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437163 (дата обращения: 31.08.2020).

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: 31.08.2020).

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 (дата обращения: 31.08.2020)

3. Брюхомицкий, Ю. А. Искусственные иммунные системы в информационной безопасности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный

университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 147 с. - ISBN 978-5-9275-3212-4. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1088177 (дата обращения: 31.08.2020)

МАКРООБЪЕКТЫ:

4. 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 31.08.2020)

5. 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 31.08.2020)

*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:

Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Тестирование систем защиты информации автоматизированных систем» (Приложение 1).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
MS Office Visio Prof 2007(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2010(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2013(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2016(для классов)	Д-1227-18 от 08.10.2018	11.10.2021

MS Office Visio Prof 2019(для	Д-1227-18 от 08.10.2018	11.10.2021
Adobe	свободно	бессрочно
MS Windows 10 Professional	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla	свободно распространяемо	бессрочно
Браузер	свободно	бессрочно
FAR	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/
Информационная система - Банк данных угроз	https://bdu.fstec.ru/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Архив научных журналов «Национальный электронно-информационный	https://archive.neicon.ru/xmlui/
Международная реферативная и полнотекстовая справочная база данных научных изданий	https://www.nature.com/siteindex
Международная реферативная база данных по чистой и	http://zbmath.org/
Международная база справочных изданий по всем	http://www.springer.com/references
Международная база научных материалов в области	http://materials.springer.com/
Международная коллекция научных протоколов по	http://www.springerprotocols.com/
Международная база полнотекстовых журналов	http://link.springer.com/
Международная реферативная и полнотекстовая справочная	http://scopus.com
Университетская информационная система	https://uisrussia.msu.ru

Федеральный образовательный портал – Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.asp
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/

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.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Тестирование систем защиты информации автоматизированных систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

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 вопросов по темам:

Перечень контрольный вопросов:

1. Определение сертификации средств защиты информации
2. Правила и участники сертификации средств защиты информации
3. Законодательно-правовые основы сертификации
4. Традиционные руководящие документы Гостехкомиссии России
5. Классы защищенности средств вычислительной техники
6. Классы защищенности межсетевых экранов
7. Классы защищенности автоматизированных систем
8. Контроль отсутствия недекларированных возможностей
9. Функциональные требования безопасности
10. Требования доверия к безопасности
11. Требования к системам обнаружения вторжений
12. Требования к средствам антивирусной защиты
13. Методики сертификационных испытаний
14. Формальный базис испытаний средств защиты информации
15. Методика проверки дискреционного принципа контроля доступа
16. Методика проверки мандатного принципа контроля доступа
17. Методика проверки механизмов очистки памяти
18. Методика проверки механизмов изоляции модулей
19. Методика проверки механизмов идентификации и аутентификации субъектов доступа
20. Методика проверки механизмов контроля целостности
21. Методика испытаний межсетевых экранов
22. Проверка механизмов фильтрации данных и трансляции адресов
23. Проверка механизмов идентификации и аутентификации администраторов
24. Проверка механизмов контроля целостности
25. Методика испытаний автоматизированных систем
26. Методика проверки механизмов идентификации и аутентификации субъектов доступа
27. Методика проверки механизмов управления доступом
28. Методика проверки механизмов контроля целостности
29. Методика проведения испытания по требованиям «Общих критериев»
30. Методики проведения аттестации ИС по требованиям защиты ПДн.
31. Цели и задачи аттестационных испытаний.
32. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ.
33. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ.
34. Условия и порядок проведения аттестационных испытаний объекта ВТ.
35. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.
36. Объем испытаний на соответствие требованиям по ЗИ от НСД.
37. Проверка ВП на соответствие организационно-техническим требованиям по защите информации.
38. Условия и порядок проведения аттестационных испытаний ВП.
39. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП.

40. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП.
41. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.

7. Оценочные 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-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем		
ПК-6.1	– Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	1. Определение сертификации средств защиты информации 2. Правила и участники сертификации средств защиты информации 3. Законодательно-правовые основы сертификации 4. Традиционные руководящие документы Гостехкомиссии России 5. Классы защищенности средств вычислительной техники 6. Классы защищенности межсетевых экранов 7. Классы защищенности автоматизированных систем 8. Функциональные требования безопасности 9. Требования доверия к безопасности 10. Требования к системам обнаружения вторжений 11. Требования к средствам антивирусной защиты – правила оформления научно-технической документации; – принципы работы и параметры используемого оборудования для проведения экспериментально-исследовательских работ; типовые схемы экспериментального исследования основных электронных приборов и устройств
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем	1. Провести тестирование механизмов фильтрации данных и трансляции адресов 2. Провести тестирование механизмов идентификации и аутентификации администраторов 3. Провести тестирование механизмов контроля целостности 4. Провести тестирование антивирусной защиты – составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия; – проводить анализ решения о проведении сертификации средства защиты информации /сертификационных испытаний для продления срока действия сертификата соответствия проводить анализ сертификата соответствия Составить план и пояснить этапы методики сертификационных испытаний 1. Составить план и пояснить этапы тестирования дискреционного принципа контроля доступа 2. Составить план и пояснить этапы тестирования мандатного принципа контроля доступа

		3. Составить план и пояснить этапы тестирования механизмов очистки памяти 4. Составить план и пояснить этапы тестирования механизмов изоляции модулей 5. Составить план и пояснить этапы тестирования механизмов идентификации и аутентификации субъектов доступа 6. Составить план и пояснить этапы тестирования механизмов контроля целостности 7. Составить план и пояснить этапы тестирования испытаний межсетевых экранов
ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах	1. Методики проведения аттестации ИС по требованиям защиты ПДн. 2. Цели и задачи аттестационных испытаний. 3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. 4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.
ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем	1. Объем испытаний на соответствие требованиям по ЗИ от НСД. 2. Проверка ВП на соответствие организационно-техническим требованиям по защите информации. 3. Условия и порядок проведения аттестационных испытаний ВП. 4. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 5. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 6. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний. – Средства анализа информационной безопасности; – Классификацию систем защиты информации; Средства организации аттестации ВП по требованиям безопасности информации 1. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации с целью дальнейшего тестирования. 2. Произвести тестирование информационных потоков 3. Определить состав использованных для обработки защищаемой информации средств ВТ и составить план тестирования. 4. Составить план проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Определить условия и порядок проведения тестирования для

		аттестации объекта ВТ. 1. Произвести тестирование защиты информации от утечки за счет ПЭМИ СВТ 2. Определить объем тестирования на соответствие требованиям по ЗИ от НСД. 3. Произвести проверку ВП на соответствие организационно-техническим требованиям по защите информации. 4. Определить условия и порядок тестирования ВП для последующей аттестации. 5. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 6. Определить объем тестирования ВП на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 7. Произвести тестирование требований по защите информации от утечки по акустическому и виброакустическому каналам для ВП.

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

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

Показатели и критерии оценивания зачета:

– на оценку **«зачтено»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

ПРИЛОЖЕНИЕ 3

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Рекомендации направлены на оказание методической помощи обучающимся при выполнении лабораторных работ.

Лабораторная работа – 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 лабораторных работ является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами лабораторных работ 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 лабораторных работ определяется рабочей программой дисциплины. План лабораторных работ отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

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

На 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. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных 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 лабораторных работ обучающийся должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

После выполнения каждой лабораторной 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 лабораторной работы оформляются в соответствии с требованиями к выполнению конкретной работы.

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.

ПРИЛОЖЕНИЕ 4

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы с обучающимися группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.