МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«26» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕСТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
наименование дисциплины

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7

Магнитогорск
2018 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«07» сентября 2018 г., протокол № 1.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«26» сентября 2018 г., протокол № 1.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: доцент кафедры ИиИБ, к.т.н.
(должность, ученая степень, ученое звание)

_____ / У.В. Михайлова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

1. **Цели освоения дисциплины**

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 в структуре образовательной программы подготовки специалиста

Дисциплина «Тестирование систем защиты информации автоматизированных систем» входит в факультативы образовательной программы.

Для изучения дисциплины необходимы знания, сформированные в результате изучения дисциплин: «Безопасность операционных систем», «Сети и системы передачи информации», «Безопасность сетей ЭВМ», «Безопасность систем баз данных», «Программно-аппаратные средства обеспечения информационной безопасности», «Организация ЭВМ и вычислительных систем»

Дисциплина является предшествующей для изучения дисциплин: «Методы мониторинга информационной безопасности АС», «Анализ безопасности программного обеспечения», «Управление информационной безопасностью», «Информационная безопасность распределенных информационных систем» и производственных практик.

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

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

Структурный элемент компетенции	**Планируемые результаты обучения**
ПК-15. Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	
Знать	– 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
Уметь	– 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.
Владеть	– терминологий в области экспериментально–исследовательских работ, а также способностью вести аргументированную дискуссию по результатам экспериментально-исследовательских работ; – нормативно-правовой базой в области сертификации средств защиты информации
ПК-16. Способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	
Знать	– Средства анализа информационной безопасности; – Классификацию систем защиты информации; – Средства организации аттестации ВП по требованиям безопасности информации.
Уметь	– Принимать участие в исследованиях аттестации системы защиты информации; – Принимать участие в исследованиях и анализе аттестации системы защиты информации; – Проводить научно-исследовательские работы при аттестации системы защиты

Структурный элемент компетенции	Планируемые результаты обучения
	информации с учетом требований к обеспечению информационной безопасности.
Владеть	– Навыками использования средств анализа информационной безопасности; – Навыками проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; – Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.

Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет **1** зачетную единицу **36** акад. часов, в том числе:

- контактная работа – 17,95 акад. часов:
  - аудиторная – 17 акад. часов;
  - внеаудиторная – 0,95 акад. часов
- самостоятельная работа – 18,05 акад. часов;

Форма аттестации: зачет

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		Лекции	Практич. Занятия				
Раздел 1. Сертификация средств защиты информации автоматизированных систем							
Тема 1.1. Общие сведения. Организационная структура системы сертификации. Подача заявки на сертификацию.	VII	2		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-15 з ПК-16 з
Тема 1.2 Принятие решения о проведении сертификации средства защиты информации. Сертификационные испытания средства защиты информации.	VII	2		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-15 зув ПК-16 зув
Тема 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,	VII	5		5	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-15 зув ПК-16 зув

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
приостановление и прекращение сертификата соответствия.							
Итого по разделу	VII	9		9			
Раздел 2. Аттестации автоматизированных систем с учетом нормативных документов по защите информации							
Тема 2.1. Общие положения. Организационная структура системы аттестации.	VII	2		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-15 з ПК-16 з
Тема 2.2. Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте. Порядок проведения аттестации и контроля	VII	2		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-15 зув ПК-16 зув
Тема 2.3 Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации.	VII	4		5,05	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-15 зув ПК-16 зув
Итого по разделу	VII	8		9,05			
Итого за семестр		**17**		**18,05**		**Промежуточная аттестация (Зачет)**	
Итого по дисциплине		**17**		**18,05**		**Промежуточная аттестация (Зачет)**	

5 Образовательные и информационные 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.

Формы учебных занятий с использованием традиционных технологий:

- ***обзорные лекции*** – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;
- ***информационные*** – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала

- ***проблемная*** - для развития исследовательских навыков и изучения способов решения задач.
- ***лекции с заранее запланированными ошибками*** – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.

Формы учебных занятий с использованием игровых технологий:

- ***Учебная игра*** **–** форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.
- ***Деловая игра*** – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Технологии проектного обучения

- ***Творческий проект*** – учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.).
- ***Информационный проект*** – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

Формы учебных занятий с использованием информационно-коммуникационных технологий:

- ***Лекция-визуализация*** – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).
- ***методы IT***
  - Организация доступа обучающихся к основным и дополнительным лекционным материалам с использованием клиент-серверных технологий (платформа e-Learning).
  - Использование электронных образовательных ресурсов для организации самостоятельной работы обучающихся. Разработка преподавателями кафедры авторских ЭОР, подготовка перечня и ориентация обучающихся на государственные образовательные интернет-ресурсы.
  - Использование в образовательном процессе электронных учебников, компьютерных обучающих систем, интерактивных упражнений.
- ***учебная дискуссия***
  - Проведение семинаров, посвященных вопросам информатики, подготовка тематических презентаций по заданным темам, и дальнейший обмен взглядами по конкретной проблеме.
- ***использование тренингов***
  - Подготовка и проведение демонстрационных, тематических и итоговых компьютерных тестирований как в качестве локальных, так и внешних контрольных мероприятий.

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-15. Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем		
Знать	– 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	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
Уметь	– 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	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

	сертификата соответствия.	
Владеть	– терминологий в области экспериментально–исследовательских работ, а также способностью вести аргументированную дискуссию по результатам экспери-ментально-исследовательских работ; – нормативно-правовой базой в области сертификации средств защиты информации	1. Составить план и пояснить этапы методики сертификационных испытаний 2. Составить план и пояснить этапы тестирования дискреционного принципа контроля доступа 3. Составить план и пояснить этапы тестирования мандатного принципа контроля доступа 4. Составить план и пояснить этапы тестирования механизмов очистки памяти 5. Составить план и пояснить этапы тестирования механизмов изоляции модулей 6. Составить план и пояснить этапы тестирования механизмов идентификации и аутентификации субъектов доступа 7. Составить план и пояснить этапы тестирования механизмов контроля целостности 8. Составить план и пояснить этапы тестирования испытаний межсетевых экранов
ПК-16. Способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации		
Знать	– Средства анализа информационной безопасности; – Классификацию систем защиты информации; – Средства организации аттестации ВП по требованиям безопасности информации.	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. 7. Объем испытаний на соответствие требованиям по ЗИ от НСД. 8. Проверка ВП на соответствие организационно-техническим требованиям по защите информации. 9. Условия и порядок проведения аттестационных испытаний ВП. 10. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 11. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 12. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.
Уметь	– Принимать участие в исследованиях аттестации системы защиты информации; – Принимать участие в исследованиях и анализе аттестации системы защиты 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-

	– Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.	техническим требованиям по защите информации объекта ВТ. 5. Определить условия и порядок проведения тестирования для аттестации объекта ВТ. 6. Произвести тестирование защиты информации от утечки за счет ПЭМИ СВТ.
Владеть	– Навыками использования средств анализа информационной безопасности; – Навыками проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; – Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.	1. Определить объем тестирования на соответствие требованиям по ЗИ от НСД. 2. Произвести проверку ВП на соответствие организационно-техническим требованиям по защите информации. 3. Определить условия и порядок тестирования ВП для последующей аттестации. 4. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 5. Определить объем тестирования ВП на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 6. 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.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - Режим доступа: http://znanium.com/bookread.php?book=405000. - Загл. с экрана. - ISBN 978-5-369-01178-2.

б) Дополнительная литература:

1. Информационная безопасность и защита информации [Текст]: учеб.пособ. / Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова, Н. Г. Шахов. - Старый Оскол: ТНТ, 2010.

2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс]: учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 101 с. - Режим доступа: http://znanium.com/bookread.php?book=463061 .- Загл. с экрана.

3. Агапов, А. В. Обработка и обеспечение безопасности электронных данных [Электронный ресурс]: учеб. пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев и др.; под ред. Д. В. Денисова. - М.: МФПУ Синергия, 2012. - 592 с. - (Сдаем госэкзамен). - Режим доступа: http://znanium.com/bookread.php?book=451354 .- Загл. с экрана. - ISBN 978-5-4257-0074-2.

в) Интернет – ресурсы:

1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.

2. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.

3. Государственная публичная научно-техническая библиотека России [Электронный ресурс] – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.

4. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. Яз. рус.

5. Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.

6. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.

7. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/.– Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение дисциплины

Тип и название аудитории	Оснащение аудитории
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: - Операционная система MS Windows - *Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021* ; - Пакет MS Office (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; - Архиватор 7zip - *GNU LGPL, бессрочная*; - Система компьютерной математики MathCad - *43813518 D-1662-13 от 22.11.2013*; - выход в Интернет.
Лаборатория программно-аппаратных средств защиты информации, ауд. 2124	Персональные компьютеры с ПО: - Операционная система MS Windows - *Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021* ;
Аудитории для самостоятельной	Персональные компьютеры с ПО:

Тип и название аудитории	Оснащение аудитории
работы (ауд.132а): компьютерные классы; читальные залы библиотеки	- Операционная система MS Windows - *Microsoft Imagine - Premium D-1227-18 от 08.10.2018 до 08.10.2021* ; - Пакет MS Office (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; - Архиватор 7zip - *GNU LGPL, бессрочная*; - Выход в Интернет и с доступ в электронную информационно-образовательную среду университета

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности *10.05.03 Информационная безопасность автоматизированных систем. Специализация «Обеспечение информационной безопасности распределенных информационных систем».*