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)

РАЗРАБОТКА ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ НА СИСТЕМЫ 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	8

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: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(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 «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» является формирование у обучающихся понятий эксплуатационной документации, формировании требований и правил обслуживания систем защиты информации, разработки и ведения эксплуатационной документации на системы защиты информации автоматизированных систем 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 «Разработка эксплуатационной документации на системы 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».

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 «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	**Планируемые результаты обучения**
ПК-21. Способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	
Знать	– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; – нормативные правовые акты в области защиты информации; – основные методы управления проектами в области информационной безопасности.
Уметь	– разрабатывать эксплуатационную документацию на систему защиты автоматизированных систем; – анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; – проводить технико-экономическое обоснование и исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности.
Владеть	– методами анализа технической документации информационной инфраструктуры автоматизированной системы; – навыком документирования программного обеспечения, технических

Структурный элемент компетенции	Планируемые результаты обучения
	средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.
ПК-23. Способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Знать	– основные меры по защите информации в автоматизированных системах; – особенности защиты информации в автоматизированных системах управления технологическими процессами; – угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах.
Уметь	– определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; – Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.
Владеть	– методами анализа защищенности информационной инфраструктуры автоматизированной системы; – навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач;

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. Техническая документация автоматизированных систем в защищенном исполнении							
Тема 1.1. Общие сведения. Назначение технической документации. Требования к технической документации	VIII	2		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-21 з ПК-23 з
Тема 1.2 Стандарты в области информационных систем. Комплекс стандартов и руководящих документов на автоматизированные системы	VIII	2		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-21 зув ПК-23 зув
Тема 1.3 Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении.	VIII	5		5	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-21 зув ПК-23 зув
Итого по разделу	VIII	9		9			
Раздел 2. Разработка							

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				
эксплуатационной документации							
Тема 2.1. Общие положения. Состав эксплуатационной документации. Виды и номенклатура эксплуатационных документов. Требования к эксплуатационной документации	VIII	4		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-21 з ПК-23 з
Тема 2.2. Составление руководства пользователя с выделением действий по обеспечению информационной безопасности.	VIII	2		2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-21 зув ПК-23 зув
Тема 2.3 Составление программы и методики испытаний системы защиты автоматизированной системы.	VIII	2		5,05	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-21 зув ПК-23 зув
Итого по разделу	VIII	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 «Разработка эксплуатационной документации на системы 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 «Разработка эксплуатационной документации на системы 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 вопросы по темам:

Перечень контрольный вопросов:

1. Жизненный цикл системы информационной безопасности
2. Стадии и этапы создания автоматизированной системы
3. Понятие эксплуатационной документации на автоматизированную систему
4. Виды документов, относящихся к эксплуатационной документации
5. Требования к управлению документами проекта
6. Основные понятия проектного менеджмента и их взаимосвязь
7. Требования при создании (модернизации) автоматизированной системы в защищенном исполнении
8. Национальные стандарты, рекомендуемые к применению при создании автоматизированных систем в защищенном исполнении
9. Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении
10. Содержание эксплуатационной документации на систему защиты автоматизированной системы
11. Содержание документа «Руководство по эксплуатации»
12. Содержание документа «Формуляр»
13. Виды испытаний автоматизированных систем
14. Виды программных документов
15. Назначение документа «Программа и методика испытаний» на систему защиты автоматизированной системы

16. Перечень проверок, подлежащих включению в программу испытаний
17. Основные разделы программы испытаний
18. Содержание документа «Общее описание системы»
19. Состав приемочных испытаний
20. Руководство пользователя системы защиты автоматизированной системы
21. Основные моменты в описании технологического процесса обработки данных в системе защиты автоматизированной системы
22. Инструкция по формированию и ведению базы данных (набора данных)
23. Составление инструкции о мерах по обеспечению информационной безопасности
24. Инструкция администратору безопасности информации автоматизированной системы

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-21. Способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем		
Знать	– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; – нормативные правовые акты в области защиты информации; – основные методы управления проектами в области информационной безопасности.	1. Перечислить национальные стандарты, рекомендуемые к применению при создании автоматизированных систем в защищенном исполнении 2. Рассказать порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении 3. Перечислить документы, относящиеся к эксплуатационной документации на систему защиты автоматизированной системы 4. Перечислить виды испытаний автоматизированных систем 5. Перечислить виды программных документов 6. Перечислить требования к управлению документами проекта 7. Рассказать об основных понятиях проектного менеджмента и установить их взаимосвязь 8. Дать определение эксплуатационной документации на автоматизированную систему
Уметь	– разрабатывать эксплуатационную документацию на систему защиты автоматизированных систем; – анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления	1. Составить перечень необходимой документации стадии «Рабочая документация», относящейся к эксплуатационной 2. Составить технологическую инструкцию для системы защиты автоматизированной системы 3. Составить руководство по эксплуатации системы защиты автоматизированной системы 4. Составить программу опытной эксплуатации для системы защиты автоматизированной системы 5. Составить схему организационной структуры управления проектами и определить взаимосвязи основных понятий проектного менеджмента

	потенциальных уязвимостей систем защиты информации автоматизированных систем; – проводить технико-экономическое обоснование и исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности.	
Владеть	– методами анализа технической документации информационной инфраструктуры автоматизированной системы; – навыком документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.	1. Составить руководство по эксплуатации комплекса технических средств системы защиты автоматизированной системы 2. На основании технического задания определить требования к составу и содержанию работ по подготовке системы защиты к вводу в действие; 3. Составить инструкцию для администратора безопасности информации автоматизированной системы; 4. Разработать инструкцию по формированию и ведению базы данных (набора данных)
ПК-23. Способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
Знать	– основные меры по защите информации в автоматизированных системах; – особенности защиты информации в автоматизированных системах управления технологическими процессами; – угрозы безопасности,	1. Описать технологический процесс обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. 2. Проверить выполнение требований по защите информации от утечки за счет ПЭМИ СВТ. 3. Перечислить испытания на соответствие требованиям по ЗИ от НСД. 4. Перечислить требования при создании (модернизации) автоматизированной системы в защищенном исполнении 5. Дать понятие политики информационной безопасности организации

	информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах.	
Уметь	– определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; – Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.	1. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации; 2. Составить инструкцию по антивирусному контролю; 3. Разработать организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам автоматизированной системы; 4. Составить предписание на эксплуатацию СВТ; 5. Составить инструкцию по эксплуатации СЗИ (по выбору) в соответствии с ГОСТ 2.610-2006
Владеть	– методами анализа защищенности информационной инфраструктуры автоматизированной системы; – навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач;	1. Составить инструкцию о мерах по обеспечению информационной безопасности 2. Составить технический паспорт на систему защиты автоматизированной системы с приложениями: a) состав технических и программных средств, входящих в систему защиты АС; b) места установки СЗИ и технических средств; c) параметры и порядок настройки средств защиты информации, программного обеспечения и технических средств.

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.

2. ГОСТ 2.610-2006 Единая система конструкторской документации (ЕСКД). Правила выполнения эксплуатационных документов. М.:Стандартинформ, 2008. – 39 с.

3. ГОСТ 34.601–90 Информационная технология. Комплекс стандартов на автоматизированные системы. Стадии создания. – М.: Изд-во стандартов, 2003. – 6 с.

4. ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем М.: Переиздание Стандартинформ, 2008. –10с.

5. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – 34с.

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 работы (ауд.132а): компьютерные классы; читальные залы библиотеки	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*; - 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».*