



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
С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

***РАЗРАБОТКА ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ НА
СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ***

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы

10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

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

Магнитогорск
2019 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой  И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель  С.И. Лукьянов

Рабочая программа составлена:

зав. кафедрой ИиИБ, д-р техн. наук  И.И. Баранкова

Рецензент:

Начальник отдела информационной безопасности «КУБ» (АО)

 М.М. Блинецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 1 сентября 2020 г. № 1
Зав. кафедрой И.И. Баранкова И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 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 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

1 Цели освоения дисциплины (модуля)

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 (модуля) в структуре образовательной программы

Дисциплина Разработка эксплуатационной документации на системы защиты информации автоматизированных систем входит в вариативную часть учебного плана образовательной программы.

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

Безопасность операционных систем

Сети и системы передачи информации

Безопасность сетей ЭВМ

Безопасность систем баз данных

Программно-аппаратные средства обеспечения информационной безопасности

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

Методы мониторинга информационной безопасности АС

Анализ безопасности программного обеспечения

Управление информационной безопасностью

Информационная безопасность систем организационного управления

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Производственная-преддипломная практика

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

В результате освоения дисциплины (модуля) «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
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	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — методами анализа защищенности информационной инфраструктуры автоматизированной системы; — навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач;
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	
Знать	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — 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.

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 1 зачетных единиц 36 академических часов, в том числе:

- контактная работа – 17,95 академических часов;
- аудиторная – 17 академических часов;
- внеаудиторная – 0,95 академических часов;
- самостоятельная работа – 18,05 академических часов;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в академических часах)			Самостоятельная работа обучающегося	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Техническая документация автоматизированных систем в защищенном исполнении								
1.1 Общие сведения. Назначение технической документации. Требования технической документации	8	2			2	поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-23, ПК-21
1.2 Стандарты в области информационных систем. Комплекс стандартов и руководящих документов на автоматизированные системы		2			2	поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-23, ПК-21

1.3 Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении.		5			5	поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-23, ПК-21
Итого по разделу		9			9			
2. Разработка эксплуатационной документации								
2.1 Общие положения. Состав эксплуатационной документации. Виды и номенклатура эксплуатационных документов. Требования к эксплуатационной документации		4			2	поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-23, ПК-21
2.2 Составление руководства пользователя с выделением действий по обеспечению информационной безопасности.	8	2			2	поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-23, ПК-21
2.3 Составление программы и методики испытаний системы защиты автоматизированной системы.		2			5,05	поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к зачету.		ПК-23, ПК-21
Итого по разделу		8			9,05			
Итого за семестр		17			18,05		зачёт	
Итого по дисциплине		17			18,05		зачет	ПК-23,ПК-21

5 Образовательные 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 компетентного 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

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 контрольных 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	<ul style="list-style-type: none"> – 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. 	<ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> – 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. 	<ol style="list-style-type: none"> 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
Владеть	– методами анализа технической	1. Составить руководство по эксплуатации комплекса технических средств системы защиты автоматизированной

	<p>документации информационной инфраструктуры автоматизированной системы;</p> <ul style="list-style-type: none"> – навыком документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации. 	<p>системы</p> <ol style="list-style-type: none"> 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)
<p>ПК-23. Способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</p>		
Знать	<ul style="list-style-type: none"> – 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. 	<ol style="list-style-type: none"> 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
Уметь	<ul style="list-style-type: none"> – 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. 	<ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> – методами анализа защищенности информационной инфраструктуры автоматизированной системы; – навыками формирования требований по защите информации, включая использование математического 	<ol style="list-style-type: none"> 1. Составить инструкцию о мерах по обеспечению информационной безопасности 2. Составить технический паспорт на систему защиты автоматизированной системы с приложениями: <ol style="list-style-type: none"> а) состав технических и программных средств, входящих в систему защиты АС; б) места установки СЗИ и технических средств; в) параметры и порядок настройки средств защиты информации, программного обеспечения и технических средств.

	аппарата для решения прикладных задач;	
--	--	--

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. 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. Защита 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.znaniium.com/catalog/product/1018901> (дата обращения: 31.08.2020)

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

с.

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

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

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

7. 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)

8. 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)

9. Баранкова И. И. , Пермякова О.В. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - ISBN 978-5-9967-1031-7 URL: <https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true> (дата обращения 31.08.2020)

в) Методические указания:

Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Разработка эксплуатационной документации на системы 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
7Zip	свободно распространяемое ПО	бессрочно
MS Office 2007 Professional	№ 135 от 17.09.2007	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 классов)	Д-1227-18 от 08.10.2018	11.10.2021
LibreOffice	свободно распространяемое	бессрочно
Adobe Reader	свободно распространяемое	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое	бессрочно
FAR Manager	свободно распространяемое	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования	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 ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.asp
Федеральный образовательный портал – Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com
Международная реферативная и полнотекстовая справочная база данных	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная коллекция научных протоколов по различным отраслям знаний	http://www.springerprotocols.com/
Международная база научных материалов в области физических наук и инжиниринга	http://materials.springer.com/
Международная база справочных изданий по всем отраслям знаний SpringerReference	http://www.springer.com/references

Международная реферативная база данных по чистой и	http://zbmath.org/
Международная реферативная и полнотекстовая справочная база данных научных изданий	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	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-i-nformatsii
Информационная система - Банк данных угроз	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;

- Выход в Интернет и с доступ в электронную информационно-образовательную

среду университета

Лаборатория программно-аппаратных средств обеспечения информационной

безопасности, ауд. 2124

- Персональные компьютеры с ПО;

- Выход в Интернет и с доступ в электронную информационно-образовательную

среду университета

Аудитории для самостоятельной работы (ауд.132а):

- Персональные компьютеры с ПО;

- Выход в Интернет и с доступ в электронную информационно-образовательную

среду университета

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.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.6) «Оценочные средства для проведения промежуточной аттестации» данной РПД.