Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

КОМПОНЕНТЫ ДОВЕРЕННОЙ АППАРАТНОЙ ПЛАТФОРМЫ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
4	3	108	6	24	0		42	0	Э
Итого	3	108	6	24	0	12	42	0	

АННОТАЦИЯ

Задачами дисциплины являются:

- дать основы первичного анализа состава радиоэлектронной аппаратуры с выделением критичных и подозрительных элементов, блоков, узлов; познакомить с существующими методами более детального анализа и проверки аутентичности электронных компонентов, блоков и узлов для развития навыков рационального выбора состава и последовательности применения этих методов, которые нарабатываются в ходе практических занятий; обоснованного разделения подозрительных электронных компонентов на аутентичные, контрафактные, а также искусственно внесенные в конструкцию для получения несанкционированного доступа к информации и/или реализации недекларированных возможностей. В основе теоретической базы лежат как отечественные нормативные документы (национальные стандарты, рекомендации), так и зарубежные стандарты, разработанные международными исследовательскими группами.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Компоненты доверенной аппаратной платформы» является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ в области выбора и применения методов выявления демаскирующих признаков неаутентичных электронных компонентов, блоков, модулей в составе радиоэлектронной аппаратуры.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Компоненты доверенной аппаратной платформы» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры»

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями, умениями и навыками смежных дисциплин «Теоретические основы защиты информации в ключевых системах информационной инфраструктуры», «Организационно-правовые механизмы обеспечения информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», «Основы аттестации объектов информатизации».

Знания, полученные при изучении дисциплины «Компоненты доверенной аппаратной платформы» являются базовыми, для дисциплин, входящих в вариативную часть профессионального цикла учебного плана подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность» по образовательной программе подготовки «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
контрольно-аналитический			
Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры	ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.034	З-ПК-4[1] - Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации

			работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения

			сертификационных испытаний; разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки

			протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	4 Семестр						
1	Первый раздел	1-8	4/12/0		25	КИ-8	З-ПК-4, У-ПК-4, В-ПК-4
2	Второй раздел	9-15	2/12/0		25	КИ-15	З-ПК-4, У-ПК-4, В-ПК-4
	Итого за 4 Семестр		6/24/0		50		

	Контрольные мероприятия за 4 Семестр				50	Э	З-ПК-4, У-ПК-4, В-ПК-4

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	4 Семестр	6	24	0
1-8	**Первый раздел**	4	12	0
1 - 2	**Тема 1. Общие вопросы по недекларированным возможностям, электронной компонентной базе, важные особенности и характеристики изделий электроники, применяемые для испытаний** Понятия: электроника, полупроводники, диэлектрики, металлы, электронная компонентная база, планарная технология изготовления микроэлектроники, диод, транзистор, микросхема интегральная, электронный модуль, радиоэлектронная аппаратура, гибридная микросхема, многокристальный модуль, корпус изделия ЭКБ, аналоговая и цифровая электроника	Всего аудиторных часов 1 Онлайн 0	 3 0	 0 0
3 - 4	**Тема 2. Основные общие правовые и практические вопросы, связанные с разработкой, применением и сертификацией ЭКБ** Понятия: головные научно-исследовательские организации в области разработки и применения ЭКБ, категории качества ЭКБ, порядок сертификации ЭКБ различных категорий качества, военное представительство, представитель заказчика, маркировка ЭКБ, особые знаки в маркировке, технические условия и datasheet, сопроводительная документация, источники доверенной информации признаков аутентичности ЭКБ	Всего аудиторных часов 1 Онлайн 0	 3 0	 0 0
5 - 6	**Тема 3. Угроза контрафакта в целом, мировые тенденции роста доли поддельных изделий. Угрозы объектам критической информационной инфраструктуры от применения контрафактных изделий ЭКБ включая известные** Понятия: контрафакт, признаки контрафакта, доля контрафакта в мировом рынке ЭКБ, известные случаи отказа американской военной и космической техники из-за контрафактных ЭКБ, источники поддельных ЭКБ,	Всего аудиторных часов 1 Онлайн 0	 3 0	 0 0

	примеры выявленных контрафактных изделий, нормативные документы по контрафакту ЭКБ, классификация методов выявления поддельных и подозрительных изделий, обратное проектирование			
7 - 8	**Тема 4. Недекларированные возможности ЭКБ** Понятия: недекларированные возможности, недокументированные возможности, несанкционированный доступ, саботаж, информативный сигнал, побочные электромагнитные излучения и наводки, основные технические средства и системы, вспомогательные технические средства и системы, электронное устройство негласного получения информации, классификация НДВ по реализации и по функциональному назначению, примеры таких устройств на основе литературных данных	Всего аудиторных часов		
		1	3	0
		Онлайн		
		0	0	0
9-15	**Второй раздел**	2	12	0
9 - 11	**Тема 5. Методы исследования ЭКБ для выявления признаков контрафакта по ГОСТ. Основные требования, характеристики установок реализации, последовательность проведения** Понятия: демаскирующие признаки, признаки контрафакта, первичная документация, маркировка, корпус, визуальный контроль, перемаркировка, замена верхнего покрытия корпуса, перешлифовка, проверка с применением растворителей, сканирующий электронный микроскоп, сканирующий акустический микроскоп, рентгеновский аппарат, рентгенологическое исследование, проверка с применением рентгеновской спектроскопии, электрические испытания 1, 2, 3, 4 уровней, декапсуляция, физический анализ	Всего аудиторных часов		
		1	4	0
		Онлайн		
		0	0	0
12 - 15	**Тема 6. Методы испытаний ЭКБ для выявления признаков контрафакта в соответствии с международными стандартами** Понятия: SAE, AS6171, уровни доверия, целевая достоверность аутентичности, уровень выявления испытательной лабораторией признаков контрафакта, подтвержденная достоверность аутентичности. Демаскирующие признаки: корпуса и маркировки, материала выводов, поверхности корпуса, кристалла, несоответствия электрическим нормам или функциональному контролю. Типы контрафакта в том числе специально модифицированное изделие с внесением НДВ с целью реализации НСД и саботажа. Методы выявления контрафакта: общие требования к визуально-оптическому осмотру, общий осмотр партии изделий, детальный осмотр, проверка перемаркировки, проверка обновления поверхности, измерение размеров образца, исследование текстуры поверхности. Не визуально-оптические методы выявления признаков контрафакта.	Всего аудиторных часов		
		1	8	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	Полное наименование
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	Темы занятий / Содержание
	4 Семестр
1 - 2	**Семинар №1:** Первичный анализ состава тренировочного изделия РЭА –идентификация элементов РЭА на основе маркировки корпусов и информационного поиска официальной документации на изделия ЭКБ. Анализ состава и выделение критичных и потенциально интересных для детального анализа элементов
3 - 4	**Семинар №2:** Проверка и обновление базовых знаний в области электроники, схемотехники, принципах конструирования аппаратуры. Разбор тренировочного изделия РЭА
5 - 6	**Семинар №3:** Контроль состава изделия РЭА и составление описи входящих в его состав элементов. Практическое занятие с тренировочным изделием РЭА
7	**Семинар №4:** Подготовка документов для проведения испытаний на выявление признаков контрафакта в ЭКБ: программы-методики испытаний, проекта протокола
8	**Практическое занятие:** Проверка знаний половины семестра. Проведение Контрольной работы №1
9 - 10	**Семинар №5:** Контроль наличия или отсутствия в составе РЭА критичных элементов, которые могут реализовать угрозу НСД или саботажа. Анализ состава РЭА с точки зрения выявления потенциальных НДВ.
11 - 12	**Семинар №6:** Проведение аутентификации ЭКБ изделия РЭА методами ГОСТ
13 - 14	**Семинар №7:** Проведение аутентификации ЭКБ изделия РЭА методами международных стандартов SAE
15	**Семинар №8:** Оценка подтвержденной достоверности аутентичности ЭКБ, по результатам испытаний комплексом методов.
15	**Практическое занятие:** Проверка знаний половины семестра. Проведение Контрольной работы №2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой

самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания. Поисковые методы; постановка познавательных задач. В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и выявления недекларированных возможностей в радиоэлектронной аппаратуре. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические занятия и семинары выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл семинаров по отработке методов выявления недекларированных возможностей и признаков контрафакта, проводится в специализированных испытательных лабораториях с предварительной настройкой необходимого оборудования. Для проведения цикла семинаров выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении семинаров необходимо отрабатывать задания, в том числе с обсуждением домашнего задания.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на семинарах.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-4	З-ПК-4	Э, КИ-8, КИ-15
	У-ПК-4	Э, КИ-8, КИ-15
	В-ПК-4	Э, КИ-8, КИ-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.</td></tr>
</table>

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Дураковский А.П. [и др.], Москва: НИЯУ МИФИ, 2014

2. ЭИ П 30 Защита персональных данных в информационных системах. Практикум : учебное пособие, Мандрица И. В., Петренко В. И., Санкт-Петербург: Лань, 2021

3. ЭИ П 84 Информационная безопасность и защита информации : учебное пособие, Прохорова О. В., Санкт-Петербург: Лань, 2021

4. ЭИ К65 Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : лабораторный практикум, Дураковский А.П. [и др.], Москва: НИЯУ МИФИ, 2013

5. ЭИ Л 14 Сертификация информационных систем : учебное пособие, Лагоша О. Н., Санкт-Петербург: Лань, 2020

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 О-75 Основы управления информационной безопасностью Кн.1, , Москва: Горячая линия - Телеком, 2018

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы - Комплексная защита объектов информатизации, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КЛР8, КЛР16 - максим.балл-25, мин. балл –15. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При не аттестации хотя бы по одному из разделов, студент не допускается к экзамену.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования

лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы - Комплексная защита объектов информатизации, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КЛР8, КЛР16 - максим.балл-25, мин. балл – 15. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При не аттестации хотя бы по одному из разделов, студент не допускается к экзамену.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и выявления недекларированных возможностей в радиоэлектронной аппаратуре. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические занятия и семинары выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл семинаров по отработке методов выявления недекларированных возможностей и признаков контрафакта, проводится в специализированных испытательных лабораториях с предварительной настройкой необходимого оборудования. Для проведения цикла семинаров выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении семинаров необходимо отрабатывать задания, в том числе с обсуждением домашнего задания.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на семинарах.

Особенности изучения разделов дисциплины

Учебная дисциплина «Компоненты доверенной аппаратной платформы» может быть охарактеризована как прикладная дисциплина технической направленности, является достаточно сложной, поскольку требует хорошей физико-математической подготовки. Необходимо глубокое знание смежных дисциплин специализации.

В процессе изучения данной программы необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов

государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

В качестве форм промежуточного (межсеместрового) контроля полученных знаний могут быть использованы письменные работы (рефераты) в сочетании с собеседованием, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Кессаринский Леонид Николаевич, к.т.н.

Рецензент(ы):

Гавдан Г.П.