МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.Г.Игнатова
«23» марта 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Программно-аппаратные средства защиты информации»

Направление подготовки – 10.03.01 «Информационная безопасность»
Направленность (профиль) – «Техническая защита информации»

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций (подкомпетенций):

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	**ОПК-9. ПАСЗИ**. Способен применять средства защиты информации от несанкционированного доступа для решения задач профессиональной деятельности	**Знания**: Состав системы защиты информации от НСД в АС. Классификацию АС. Требования по защите информации от НСД для АС различных классов. Классификацию межсетевых экранов (МЭ). Требования к различным классам защищенности МЭ. Системы обнаружения и предупреждения сетевых вторжений. Программные и программно-аппаратных средств защиты информации от НСД в АС на базе автономного АРМ. Программные и программно-аппаратные межсетевые экраны. Программные и программно-аппаратные средства обнаружения вторжений. Средства создания виртуальных защищенных сетей. **Умения**: - выполнять основные операции по применению программно-аппаратных и программных средств защиты информации для решения задач профессиональной деятельности. **Опыт деятельности**: проведения работ по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа.
ОПК-3.2. Способен проводить работы по установке, настройке, испытаниям и	**ОПК-3.2.ПАСЗИ**. Способен проводить работы по установке, настройке, испытаниям	**Знания**: Состав системы защиты информации от НСД в АС. Классификацию АС. Требования по

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
техническому обслуживанию средств защиты информации от несанкционированного доступа	и техническому обслуживанию средств защиты информации от несанкционированного доступа	защите информации от НСД для АС различных классов. Классификацию межсетевых экранов (МЭ). Требования к различным классам защищенности МЭ. Системы обнаружения и предупреждения сетевых вторжений. Программные и программно-аппаратных средств защиты информации от НСД в АС на базе автономного АРМ. Программные и программно-аппаратные межсетевые экраны. Программные и программно-аппаратные средства обнаружения вторжений. Средства создания виртуальных защищенных сетей. **Умения**: - выполнять основные операции по применению программно-аппаратных и программных средств защиты информации для решения задач профессиональной деятельности. **Опыт деятельности**: проведения работ по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа.
ОПК-3.4. Способен проводить контроль защищенности информации от несанкционированного доступа	-	**Знания:** Состав системы защиты информации от НСД в АС на базе автономного АРМ. Классификацию АС. Требования по защите информации от НСД для АС различных классов. Состав системы защиты информации от несанкционированного доступа в локальных и корпоративных сетях. Классификацию межсетевых экранов (МЭ). Требования к различным клас-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		сам защищенности МЭ. Системы обнаружения и предупреждения сетевых вторжений. Основные требования по защите автоматизированных систем обработки информации, составляющей государственную тайну. Основные требования по защите информационных систем персональных данных. Основные требования по защите государственных информационных систем общего пользования. Программные и программно-аппаратных средств защиты информации от НСД в АС на базе автономного АРМ. Программные и программно-аппаратные межсетевые экраны. Программные и программно-аппаратные средства обнаружения вторжений. Средства создания виртуальных защищенных сетей. Средства контроля защищенности информации от несанкционированного доступа. Сканеры безопасности. **Уметь:** Проводить контроль защищенности информации от несанкционированного доступа **Иметь опыт деятельности:** Проведения контроля защищенности АС от несанкционированного доступа к информации.

В результате изучения дисциплины студент должен:

Знать:

- Состав системы защиты информации от НСД в АС на базе автономного АРМ.
- Показатели защищенности СВТ от несанкционированного доступа к информации. Требования к показателям защищенности СВТ различных классов.

- Классификацию АС. Требования по защите информации от НСД для АС различных классов.
- Состав системы защиты информации от несанкционированного доступа в локальных и корпоративных сетях.
- Классификацию межсетевых экранов (МЭ). Требования к различным классам защищенности МЭ.
- Системы обнаружения и предупреждения сетевых вторжений.
- Основные требования по защите автоматизированных систем обработки информации, составляющей государственную тайну.
- Основные требования по защите информационных систем персональных данных.
- Основные требования по защите государственных информационных систем общего пользования.
- Требования к составу и содержанию функций защиты информации для конкретных сервисов безопасности: антивирусных средств, средств доверенной загрузки и средств предупреждения сетевых вторжений.
- Типовой состав и назначение средств защиты ОС и СУБД.
- Средства антивирусной защиты.
- Средств аутентификации.
- Средства доверенной загрузки.
- Программные и программно-аппаратных средств защиты информации от НСД в АС на базе автономного АРМ.
- Программные и программно-аппаратные межсетевые экраны.
- Программные и программно-аппаратные средства обнаружения вторжений.
- Средства создания виртуальных защищенных сетей.
- Средства контроля защищенности информации от несанкционированного доступа.
- Сканеры безопасности.

Уметь:

- Применять программно-аппаратные средства защиты информации для решения задач профессиональной деятельности.
- Проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа.
- Проводить контроль защищенности информации от несанкционированного доступа.

Иметь опыт деятельности:

- Проведения работ по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа.
- Проведения контроля защищенности АС от несанкционированного доступа к информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Программно-аппаратные средства защиты информации» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и читается на

4-м курсе в 7-м семестре.

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении следующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Защита информации от несанкционированного доступа».

Знания и умения, полученные в результате изучения дисциплины, используются в дисциплине «Основы управления информационной безопасностью», учебной, производственной практиках и при подготовке ВКР.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа, часы					Самостоятельная работа, часы	Вид промежуточной аттестации
				ВСЕГО	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации		
4	7	5	180	96	32	32	16	16	48	Экз. (36)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля (раздела)	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации		
1. Системы защиты информации от несанкционированного доступа. Требования к защищенности автоматизированных систем.	8	-	8	6	8	Компьютерный тест КТ- 1. Зачет по Лр 1 - 3

Номер и наименование модуля (раздела)	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации		
2. Программные и программно-аппаратные средства защиты информации от несанкционированного доступа.	20	24	4	6	28	Компьютерный тест КТ- 2. Зачет по Лр 4 – 7
3. Средства контроля защищенности информации от несанкционированного доступа.	4	8	4	4	12	Компьютерный тест КТ- 3. Зачет по Лр 8, 9

4.1. Лекционные занятия

Номер модуля дисциплины	**Номер лекции**	**Объем занятий, часы**	**Краткое содержание**
1.	1.	2	**Лекция 1. Системы защиты информации от несанкционированного доступа (НСД) в автоматизированной системе (АС) на базе автономного автоматизированного рабочего места (АРМ).** Состав системы защиты информации от НСД в АС на базе автономного АРМ. Показатели защищенности СВТ от несанкционированного доступа к информации. Требования к показателям защищенности СВТ различных классов. Классификация АС. Требования по защите информации от НСД для АС различных классов.
	2.	2	**Лекция 2. Системы защиты информации от несанкционированного доступа в локальных и корпоративных сетях.** Состав системы защиты информации от несанкционированного доступа в локальных и корпоративных сетях. Классификация межсетевых экранов (МЭ).

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			Требования к различным классам защищенности МЭ. Системы обнаружения и предупреждения сетевых вторжений.
	3.	2	**Лекция 3. Основные требования по защите автоматизированных систем от несанкционированного доступа к информации** Основные требования по защите автоматизированных систем обработки информации, составляющей государственную тайну. Основные требования по защите информационных систем персональных данных. Основные требования по защите государственных информационных систем общего пользования.
	4.	2	**Лекция 4. Критерии оценки безопасности информационных технологий (ГОСТ 15408).** Основные положения и понятия «Общих критериев», функции безопасности, профиль защиты, функции доверия, оценочные уровни, верификация выполнения требований. Требования к составу и содержанию функций защиты информации для конкретных сервисов безопасности: антивирусных средств, средств доверенной загрузки и средств предупреждения сетевых вторжений.
2.	5.	4	**Лекция 5. Программные средства защиты в составе операционных систем и систем управления базами данных.** Типовой состав и назначение средств защиты ОС и СУБД, установка и управление их функционированием (настройка).
	6.	2	**Лекция 6. Антивирусные программы.** Сертифицированные средства антивирусной защиты. Средства антивирусной защиты иностранного производства.
	7.	2	**Лекция 7. Программно-аппаратные средства аутентификации и доверенной загрузки.** Типы программно-аппаратных средств аутентификации. Обзор современных средств аутентификации. Типы средств доверенной загрузки. Обзор современных программно-аппаратных средств доверенной загрузки.
	8.	4	**Лекция 8. Программные и программно-аппаратные средства защиты информации от несанкционированного доступа в АС на базе автономного АРМ.** Типовой состав и назначение средств защиты информации от НСД. Обзор современных программно-аппаратных средств защиты информации от НСД в АС на базе автономного АРМ.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	9.	4	**Лекция 9. Программные и программно-аппаратные средства сетевой безопасности.** Программные и программно-аппаратные межсетевые экраны. Программные и программно-аппаратные средства обнаружения вторжений.
	10.	4	**Лекция 10. Средства создания виртуальных защищенных сетей.** «VipNet». С-Терра VPN.
3.	11.	2	**Лекция 11. Средства контроля защищенности информации от несанкционированного доступа.** Средство фиксации и контроля исходного состояния программного комплекса "ФИКС". Средство создания модели системы разграничения доступа "Ревизор 1 XP". Средство контроля защищенности от несанкционированного доступа "Ревизор 2 XP". Программа поиска и гарантированного уничтожения информации на дисках "TERRIER.
	12.	2	**Лекция 12. Сканеры безопасности.** Сканер безопасности «Сканер-ВС». Сканер безопасности «Ревизор сети». Сканер безопасности XSpaider.

4.2. Практические занятия

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
1.	1.	4	**Практическое занятие (семинар). Основные требования по защите автоматизированных систем от несанкционированного доступа к информации** Основные требования по защите автоматизированных систем обработки информации, составляющей государственную тайну.

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
			Основные требования по защите информационных систем персональных данных. Основные требования по защите государственных информационных систем общего пользования.
	2.	4	**Практическое занятие (семинар). Основные требования к средствам защиты информации от несанкционированного доступа.** Профили защиты средств доверенной загрузки. Профили защиты средств антивирусной защиты. Профили защиты систем обнаружения вторжений. Требования по уровню контроля отсутствия недекларированных возможностей.
2	3.	4	**Практическое занятие (семинар). Программные и программно-аппаратные средства защиты информации от несанкционированного доступа.** Программные средства защиты информации от несанкционированного доступа в АС на базе автономного АРМ. Программно-аппаратные средства защиты информации от несанкционированного доступа в АС на базе автономного АРМ. Программные и программно-аппаратные межсетевые экраны и средства обнаружения атак.
3	4.	4	**Практическое занятие (семинар). Организация и проведения контроля защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа.** Порядок организации контроля защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа. Порядок проведения аттестационных испытаний АС на соответствие требованиям по защите информации от несанкционированного доступа. Протокол оценки защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа.

4.3. Лабораторные работы
(практическая подготовка при проведении лабораторных работ)

Номер модуля дисциплины	Номер лабораторного занятия	Объем занятий, часы	Краткое содержание
2.	1.	4	Установка и настройка программных средств защиты АС на базе АРМ (ОС Windows (7, 8), «Фикс»).
	2.	4	Установка и настройка средств антивирусной защиты (Касперский, Доктор Веб, McAfee).
	3.	4	Установка и настройка программного комплекса защиты АС на базе АРМ от несанкционированного доступа к информации «Панцирь».
	4.	8	Установка и настройка программного комплекса для организации защищенных виртуальных сетей и распределенного межсетевого экранирования «Застава».
	5.	4	Установка и настройка программно-аппаратного комплекса для обеспечения сетевой безопасности корпоративной сети С-Терра CSP VPN.
3.	6.	4	Контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа с использованием средств контроля защищенности «Ревизор 1», «Ревизор 2», «TERRIER», «ФИКС».
	7.	4	Контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа с использованием сканеров безопасности «Сканер-ВС», «Ревизор сети», «Xspider».

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	2	**Подготовка к практическому занятию (семинару) № 1.** Изучение материалов лекции 1-2 и рекомендованной литературы. Изучение плана проведения семинара 1. Подготовка доклада и презентации по одному из вопросов семинара
	2	**Подготовка к практическому занятию (семинару) № 2.** Изучение материалов лекции 3-4 и рекомендованной литературы. Изучение плана проведения семинара 2. Подготовка доклада и презентации по одному из вопросов семинара
	4	**Подготовка к компьютерному тесту КТ-1.** Изучение материалов лекции 1-4 и рекомендованной литературы.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
2	4	**Подготовка к практическому занятию (семинару) № 3.** Изучение материалов лекции № 5 - 10 и рекомендованной литературы. Изучение плана проведения семинара 3. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к лабораторной работе № 1** Изучение материалов лекции №№ 5 - 10 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 1.
	4	**Подготовка к лабораторной работе № 2** Изучение материалов лекции №№ 5 - 10 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 2.
	4	**Подготовка к лабораторной работе № 3** Изучение материалов лекции №№ 5 - 10 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 3.
	4	**Подготовка к лабораторной работе № 4** Изучение материалов лекции №№ 5 - 10 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 4.
	6	**Подготовка к лабораторной работе № 5** Изучение материалов лекции №№ 5 - 10 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 5.
	2	**Подготовка к компьютерному тесту КТ-2.** Изучение материалов лекции № 5-10 и рекомендованной литературы.
3	2	**Подготовка к практическому занятию (семинару) № 4:** Изучение материалов лекции № 11- 12 и рекомендованной литературы. Изучение плана проведения семинара 4. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к лабораторной работе № 6** Изучение материалов лекции №№ 11 - 12 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 6.
	4	**Подготовка к лабораторной работе № 7** Изучение материалов лекции №№ 11 - 12 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 7.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
	2	**Подготовка к компьютерному тесту КТ-3.** Изучение материалов лекции 11-12 и рекомендованной литературы.

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС, http://orioks.miet.ru/):

Модуль 1. «Системы защиты информации от несанкционированного доступа. Требования к защищенности автоматизированных систем»:

Тексты лекций № 1 – 4. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения семинарских занятий № 1 и 2. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. «Программные и программно-аппаратные средства защиты информации от несанкционированного доступа»:

Тексты лекций № 5 – 10. ОРИОКС// URL: http://orioks.miet.ru/

План проведения семинарского занятия № 3. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 1 – 5. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 3. «Средства контроля защищенности информации от несанкционированного доступа»:

Тексты лекций № 11 – 12. ОРИОКС// URL: http://orioks.miet.ru/

План проведения семинарского занятия № 4. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 6 и 7. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Мельников, Д.А. Информационная безопасность открытых систем : учебник /Д.А. Мельников. - Москва: Флинта: Наука, 2014. - 448 с. - URL: https://e.lanbook.com/book/48368 (дата обращения: 15.03.2021). - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7.

2. Программно-аппаратные средства защиты информации: учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1.

3. Программно-аппаратные средства защиты информации: учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5 .

4. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8 .

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ: с изм. на 02 июля 2021 г.- «Об информации, информационных технологиях и о защите информации»; Текст: электронный // Техэксперт : [сайт]. – URL: https://docs.cntd.ru/document/901990051. - (дата обращения 15.03.2021).

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ: (ред. от 02.07.2021) «О персональных данных»; Текст: электронный // Техэксперт : [сайт]. https://docs.cntd.ru/document/573249803?marker=64U0IK - (дата обращения 15.03.2021).

3. Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 30.11.2020) "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации".

4. Постановление Правительства РФ от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (ред. от 30.11.2020).

5. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

6. Методический документ. Методика оценки угроз безопасности информации. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2021 г. (утверждена ФСТЭК России 5 февраля 2021 г.)

7. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г.

8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.

9. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.

10. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

11. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

12. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

13. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

14. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Общие положения; Национальный стандарт РФ : Введ. 09.02.1995: М.: Издательство стандартов (Переиздание) Стандартинформ, август 2006 -URL: https://docs.cntd.ru/document/1200004675 (дата обращения: 15.03.2021) -Текст: электронный.

15. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения; Protection of information. Basic terms and definitions: Национальный стандарт РФ: Введ. 01.02.2008:М.: Стандартинформ, 2008, -URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 15.03.2021)-Текст: электронный.

16. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения Protection of information. Object of informatisation. Factors influencing the information. General: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, (Переиздание) 2018. -URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 16.03.2021) -Текст: электронный.

17. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Information protection. Sequence of protected operational system formation. General provisions; Национальный стандарт РФ: Введ. 01.09.2014.- М.: Стандартинформ, (Переиздание) октябрь 2018. -URL: https://docs.cntd.ru/document/1200108858 (дата обращения: 10.03.2021)- Текст: электронный.

18. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации Information technologies. Basic terms and definitions in scope of technical protection of information, Национальный стандарт РФ: Введ. 01.01.2006.- М.: Стандартинформ, 2018.-12 л. -Текст: непосредственный.

19. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения: Technical information protection. Terms and definitions Национальный стандарт РФ: Введ. 01.06.2006.- М.: Стандартинформ, 2006.-20 л.-Текст: непосредственный.

Периодические издания

1. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.mephi.ru/index.php/bit/index (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.
2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011 - 2018. - URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.
3. Information Security / Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Режим доступа: свободный.
4. Журнал «Вопросы кибербезопасности». – URL: http://cyberrus.com/ (дата обращения: 15.03.2021). – Режим доступа: свободный.
5. Защита информации. Inside : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 10.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный
6. «Jet Info». /Издатель: компания «Инфосистемы Джет». – URL: http://www.jetinfo.ru (дата обращения: 15.03.2021). – Режим доступа: свободный.
7. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.
3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.
4. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 10.03.2021). - Текст: электронный.
5. Бюро научно-технической информации «Техника для спецслужб». – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Режим доступа: свободный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, которое основано на интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий формами и видами взаимодействия в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС http://orioks.miet.ru.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: ОРИОКС «Домашние задания», электронная почта преподавателя.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы (http://orioks.miet.ru).

Тестирование проводится в ОРИОКС (MOODLe).

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Мультимедийное оборудование: компьютер с программным обеспечением, возможностью подключения к сети Интернет и обеспечением доступа в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (микрофон, звуковые колонки), вебкамера с микрофоном). Учебная доска.	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).
Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью»	1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120	1. Операционная система Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL (Из реестра МИЭТ п.18) –

	USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	28 шт. 3. Корпоративная информационно - технологическая платформа ОРИОКС (Из реестра МИЭТ п.88) – 28 шт.
Помещение для самостоятельной работы обучающихся: Учебная аудитории № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal 4. Корпоративная информационно - технологическая платформа ОРИОКС

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-9. ПАСЗИ. «Способен применять средства защиты информации от несанкционированного доступа для решения задач профессиональной деятельности».

ФОС по подкомпетенции ОПК-3.2.ПАСЗИ. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа

ФОС по компетенции ОПК-3.4. Способен проводить контроль защищенности информации от несанкционированного доступа

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/**.**

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В целях практической подготовки в дисциплине предусмотрены практические занятия (семинары) и лабораторные работы.

Каждая лабораторная работа направлена на формирование отдельных умений, необходимых для формирования общепрофессиональных и профессиональных компетенции.

Лабораторные работы выполняются каждым студентом индивидуально. По результатам выполнения каждой лабораторной работы студент оформляет и представляет отчет. При защите отчетов по лабораторным работам и домашних заданий преподаватель разбирает типовые ошибки и указывает их причины.

Практические занятия (семинары) проводятся в составе группы. Каждый студент готовит доклад и презентацию по одному из вопросов семинара.

Одной из форм обучения является ***консультация*** у преподавателя. Обращаться к помощи преподавателя следует в любом случае, когда студенту не ясно изложение какого-либо вопроса в учебной литературе или требуется помощь в подборе необходимой дополнительной литературы.

11.1. Методические указания студентам по подготовке к семинарам

Семинар - развернутая беседа с обсуждением доклада. Проводится на основе заранее разработанного плана, по вопросам которого готовится вся учебная группа. Основными компонентами такого занятия являются: вступительное слово преподавателя, доклады обучаемых, вопросы докладчикам, выступления студентов по докладу и обсуждаемым вопросам, заключение преподавателя.

Развернутая беседа позволяет вовлечь в обсуждение проблем наибольшее число обучаемых. Главная задача преподавателя при проведении такого семинарского занятия состоит в использовании всех средств активизации: постановки хорошо продуманных, четко сформулированных дополнительных вопросов, умелой концентрации внимания на наиболее важ-

ных проблемах, умения обобщать и систематизировать высказываемые в выступлениях идеи, сопоставлять различные точки зрения, создавать обстановку свободного обмена мнениями. Данная форма семинара способствует выработке у обучаемых коммуникативных навыков.

Как правило, темы докладов разрабатываются преподавателем заранее и включаются в планы семинаров. Доклад носит характер краткого (10-15 мин.) аргументированного изложения одной из центральных проблем семинарского занятия с использованием презентации.

11.2. Методические указания студентам по подготовке к лабораторным работам

Выполнение студентами лабораторных работ направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Ведущей дидактической целью лабораторных работ является формирование практических умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности.

Наряду с ведущей дидактической целью в ходе выполнения заданий у студентов формируются практические умения и навыки обращения с различными приборами, установками, лабораторным оборудованием, аппаратурой, которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты).

Лабораторная работа как вид учебного занятия проводиться в специально оборудованных учебных лабораториях. Продолжительность - не менее двух академических часов. Необходимыми структурными элементами лабораторной работы, помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

По каждой лабораторной работе разработаны и утверждены методические указания по их проведению.

Лабораторные работы носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Формы организации студентов на лабораторных работах: индивидуальная, при которой каждый студент выполняет индивидуальное задание.

Для проведения лабораторных работ преподавателями разрабатываются методические рекомендации по их выполнению, которые рассматриваются и утверждаются на заседании кафедры. Методические рекомендации разрабатываются по каждой лабораторной работе, предусмотренными рабочей программой учебной дисциплины: в соответствии с коли-

чеством часов, требованиями к знаниям и умениям, темой практических занятий и лабораторных работ, установленными рабочей программой учебной дисциплины по соответствующим разделам (темам).

Методические рекомендации по выполнению лабораторных работ включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на лабораторную работу;
- наименование темы лабораторной работы;
- цель лабораторной работы (в т.ч. требования к знаниям и умениям студентов, которые должны быть реализованы);
- перечень необходимых средств обучения (оборудование, материалы и др.);
- требования по теоретической готовности студентов к выполнению лабораторных работ (требования к знаниям, перечень дидактических единиц);
- содержание заданий;
- рекомендации (инструкции) по выполнению заданий;
- требования к результатам работы, в т.ч. к оформлению;
- критерии оценки и формы контроля;
- список рекомендуемой литературы;
- приложения.

При подготовке к лабораторной работы студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к лабораторной работе;
- ознакомиться с методическими рекомендации по выполнению лабораторной работы;
- прочитать конспект лекций и соответствующие главы учебника (учебного пособия), дополнить запись лекций выписками из него;
- прочитать дополнительную литературу, рекомендованную преподавателем. Наиболее интересные мысли следует выписать;
- сформулировать и записать развернутые ответы на вопросы для подготовки к лабораторной работе;
- изучить схемы лабораторных установок (стендов), порядок работы на аппаратуре и технике, правила и меры безопасности;
- подготовить отчеты для заполнения.

На лабораторной работе студент должен выполнить задание в соответствии с методическими указаниями.

Особое внимание уделить усвоению порядка проведения измерений с использованием контрольно-измерительного оборудования, составу лабораторных установок (стендов).

Отчет о лабораторной работе должен быть оформлен в соответствии методическими указаниями и ГОСТами.

При защите отчета о лабораторной работе убедительно четко и аргументировано изложить содержание проведенных исследований и выводы по полученным результатам.

По завершению занятия студент должен уяснить недостатки, указанные преподавателем при необходимости записать их содержание.

Студенты, по каким-либо причинам, отсутствовавшие на занятии, в свободное время должны самостоятельно изучить учебный материал и провести лабораторные исследования, после чего отчитаться в проделанной работе перед преподавателем.

Студенты на лабораторной работе обязаны соблюдать меры безопасности при работе

на аппаратуре (оборудовании). Перед началом занятий, каждый студент должен пройти инструктаж по соблюдению мер безопасности на рабочем месте и уяснить места расположения средств пожаротушения и обесточивания аппаратуры (оборудования).

11.3. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительно-бальная система.

Под накопительно-бальной системой понимается система количественной, балльно - рейтинговой оценки качества освоения учебной дисциплины студентом $R_{нак}$ по суммарному результату текущего $R_{тек}$ и итогового контроля $R_{итог}$, с учетом посещаемости студентом занятий, его активности на занятиях и качества выполнения им текущих заданий $R_{пр}$.

Выполнение контрольных мероприятий текущего контроля (сдача компьютерных тестов, защита отчетов по лабораторным работам, доклады на семинарских занятиях), посещаемость занятий и активность на занятиях, результаты итогового контроля (сдача экзамена) оцениваются баллами, общая сумма которых составляет 100 баллов (максимальное значение нормативного рейтинга учебной дисциплины – $R_{нор}$).

Примерная структура и график контрольных мероприятий приведены в таблице 11.1.

Таблица 11.1

Структура и график контрольных мероприятий

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
2	Практическое занятие (семинар) № 1	4	2
4	Практическое занятие (семинар) № 2	4	2
4	Компьютерный тест (КТ-1)	4	2
7	Практическое занятие (семинар) № 3	4	2
8	Лабораторная работа № 1	6	3
9	Лабораторная работа № 2	6	3
10	Лабораторная работа № 3	6	3
11	Лабораторная работа № 4	6	3
12	Лабораторная работа № 5	6	3
12	Компьютерный тест (КТ-2)	4	2
14	Практическое занятие (семинар) № 4	4	2
15	Лабораторная работа № 6	6	3
16	Лабораторная работа № 7	6	3
16	Компьютерный тест (КТ-3)	4	2
16	Посещаемость, активность	4	2
	Итого за текущий контроль	***74***	***37***
	Итоговый контроль	***26***	***13***
	Накопленный рейтинг	**100**	**50**

В экзаменационную ведомость и зачетную книжку вносится не экзаменационная оценка по дисциплине, а ***итоговая 5-балльная оценка*** за семестр, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля учеб-

ной дисциплины.

Итоговая оценка студенту по дисциплине за семестр по 5-ти балльной шкале выставляется на основе накопленной им общей суммы баллов $R_{нак}$ по итогам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Положительная оценка («отлично», «хорошо», «удовлетворительно») заносится в экзаменационную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в экзаменационную ведомость.

РАЗРАБОТЧИК

Профессор кафедры «Информационная безопасность»
доктор технических наук, доцент _____ / Душкин А.В. /

Рабочая программа дисциплины «Программно-аппаратные средства защиты информации» по направлению подготовки 10.03.01 «Информационная безопасность», направленности (профилю) «Техническая защита информации» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры 17 марта 2021 года, протокол № 3.

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А.Хорев

Лист согласования

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества

Начальник АНОК _____ / И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ

Директор библиотеки _____ / Т.П.Филиппова /