Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.30**
Трудоемкость в зачетных единицах:	**5 семестр - 4; 6 семестр - 5; всего - 9**
Часов (всего) по учебному плану:	**324 часа**
Лекции	**5 семестр - 32 часа; 6 семестр - 28 часа; всего - 60 часов**
Практические занятия	**5 семестр - 32 часа; 6 семестр - 42 часа; всего - 74 часа**
Лабораторные работы	**5 семестр - 16 часов; 6 семестр - 28 часа; всего - 44 часа**
Консультации	**6 семестр - 2 часа;**
Самостоятельная работа	**5 семестр - 63,7 часа; 6 семестр - 79,5 часа; всего - 143,2 часа**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: Контрольная работа	
Промежуточная аттестация:	
Зачет с оценкой Экзамен	**5 семестр - 0,3 часа; 6 семестр - 0,5 часа; всего - 0,8 часа**

Москва 2021

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Поляк Р.И. Идентификатор: Rbc0e923e-PoliakRI-10208dd2	Р.И. Поляк
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: освоение профессиональных компетенций по формированию готовности студентов разрабатывать системы защиты информации на основе применения методов и средств программно-аппаратной защиты информации

Задачи дисциплины

- сформировать у студентов системные теоретические знания и практические навыки по организации и технологии программно-аппаратной защиты информации.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ОПК-1.3 способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ИД-1$_{ОПК-1.3}$ Разрабатывает порядок применения программного обеспечения с целью соблюдения требований по защите информации	знать: - Типовые программные и программно-аппаратные средства резервирования и восстановления информации в автоматизированных системах; - Способы обнаружения и идентификации инцидентов информационной безопасности в процессе эксплуатации автоматизированной системы. уметь: - Проводить установку и настройку программных и программно-аппаратных средства резервирования и восстановления информации в автоматизированных системах; - Администрировать системы обнаружения и идентификации инцидентов информационной безопасности в процессе эксплуатации автоматизированной системы.
ОПК-1.4 способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ИД-1$_{ОПК-1.4}$ Контролирует корректность функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях в соответствии с нормативными и корпоративными требованиями	знать: - Особенности проведения работ по установке, настройке, администрированию, обслуживанию и проверке работоспособности программно-аппаратных и технических средств защиты информации в автоматизированных системах; - Способы осуществления диагностики и мониторинга систем защиты автоматизированных систем. уметь: - Применять типовые программно-аппаратные средства защиты информации в автоматизированных системах и базах данных;

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		- Выполнять оценку защищенности информации, идентификацию и ликвидацию инцидентов информационной безопасности в процессе эксплуатации автоматизированных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность компьютерных систем (продвинутый уровень) (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 9 зачетных единиц, 324 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Введение	32	5	8	6	8	-	-	-	-	-	10	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Введение" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Введение" подготовка к выполнению заданий на практических занятиях ***Изучение материалов литературных источников:*** [4], 1-48
1.1	Концептуальные основы информационной безопасности	16		4	4	4	-	-	-	-	-	4	-	
1.2	Основные понятия программно-аппаратной защиты информации	16		4	2	4	-	-	-	-	-	6	-	
2	Обеспечение доступности информации применением средств программно-аппаратной защиты	54		14	6	14	-	-	-	-	-	20	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Обеспечение доступности информации применением средств программно-аппаратной защиты" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Обеспечение доступности информации применением средств программно-аппаратной защиты" ***Изучение материалов литературных источников:*** [2], 14-88
2.1	Обеспечение доступности информации средствами операционной системы Управление правами доступа к ресурсам в операционных системах семейства MS Windows.	16		4	2	4	-	-	-	-	-	6	-	

	Учетные записи пользователей и групп. Управление доступом и глобальными параметрами. Основные сведения об учетных записях групп. Оснастка "Локальные пользователи и группы"													
2.2	Обработка информации на рабочих станциях и обеспечение ее доступности	18		4	2	4	-	-	-	-	-	8	-	
2.3	Обеспечение доступности информации в локальных сетях	20		6	2	6	-	-	-	-	-	6	-	
3	Обеспечение целостности информации с помощью программных и аппаратных средств	40		10	4	10	-	-	-	-	-	16	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Обеспечение целостности информации с помощью программных и аппаратных средств"
3.1	Терминология резервирования. Оперативное и автономное резервирование. Типы резервирования. Виды RAID-массивов. Исходные типы RAID-массивов. RAID-контроллеры. Основы резервирования	18		4	2	4	-	-	-	-	-	8	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Обеспечение целостности информации с помощью программных и аппаратных средств" подготовка к выполнению заданий на практических занятиях ***Изучение материалов литературных источников:*** [1], 112-201

	данных. Варианты резервирования данных													
3.2	Обеспечение целостности при передаче информации по сетям	22		6	2	6	-	-	-	-	-	8	-	
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	**144.0**		**32**	**16**	**32**	-	-	-	-	**0.3**	**46**	**17.7**	
	Итого за семестр	**144.0**		**32**	**16**	**32**	-		-		**0.3**	**63.7**		
4	Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений	58	6	12	12	16	-	-	-	-	-	18	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений" подготовка к выполнению заданий на практических занятиях ***Изучение материалов литературных источников:*** [4], 76-154 [5], 38-91
4.1	Механизмы обеспечения конфиденциальности доступа к информации на уровне операционных систем	12		2	2	4	-	-	-	-	-	4	-	
4.2	Механизмы обеспечения конфиденциальности доступа к информации на уровне приложений	12		2	2	4	-	-	-	-	-	4	-	
4.3	Программно-аппаратные средства криптографической защиты информации	16		4	4	4	-	-	-	-	-	4	-	
4.4	Обеспечение конфиденциальности информации в IP-сетях	18		4	4	4	-	-	-	-	-	6	-	

5	Комплексные системы защиты информации	42		8	8	12	-	-	-	-	-	14	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Комплексные системы защиты информации" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Комплексные системы защиты информации" подготовка к выполнению заданий на практических занятиях ***Изучение материалов литературных источников:*** [3], 5-46
5.1	Обеспечение антивирусной защиты информационных систем	12		2	2	4	-	-	-	-	-	4	-	
5.2	Предотвращение утечек информации (DLP) и учет рабочего времени	12		2	2	4	-	-	-	-	-	4	-	
5.3	Системы обнаружения и предотвращения вторжений	18		4	4	4	-	-	-	-	-	6	-	
6	Основы веб-безопасности	44		8	8	14	-	-	-	-	-	14	-	***Изучение материалов литературных источников:*** [3], 69-115
6.1	Цели атаки на веб-ресурсы предприятия	12		2	2	4	-	-	-	-	-	4	-	
6.2	Методы и инструменты злоумышленника для атаки на веб-ресурсы	12		2	2	4	-	-	-	-	-	4	-	
6.3	Классификация сетевых атак.	20		4	4	6	-	-	-	-	-	6	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**28**	**28**	**42**	-	**2**	-	-	**0.5**	**46**	**33.5**	
	Итого за семестр	**180.0**		**28**	**28**	**42**	**2**		-		**0.5**	**79.5**		
	ИТОГО	**324.0**	-	**60**	**44**	**74**	**2**		-		**0.8**	**143.2**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Введение

1.1. Концептуальные основы информационной безопасности

Основные понятия и определения в сфере информационной безопасности. Угрозы информации. Анализ методов и средств защиты информации..

1.2. Основные понятия программно-аппаратной защиты информации

Предмет и задачи программно-аппаратной защиты информации. Основные критерии оценки безопасности систем. Система организационных и руководящих документов РФ в области программно-аппаратной защиты информации..

2. Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений

2.1. Механизмы обеспечения конфиденциальности доступа к информации на уровне операционных систем

Понятия аутентификации и авторизации. Общие принципы. Задачи протокола аутентификации. Локальная и доменная регистрация. Протоколы аутентификации Windows. Автоматическая генерация и назначение сложных паролей в MS Windows.

2.2. Механизмы обеспечения конфиденциальности доступа к информации на уровне приложений

Обеспечение конфиденциальности электронных документов с использованием возможностей приложений MS Office. Защита документов MS Word и MS Excel. Защита VBA-макросов. Применение паролей MS Access и MS Outlook. Анализ уязвимостей системы защиты документов в приложениях MS Office.

2.3. Программно-аппаратные средства криптографической защиты информации

Полностью контролируемые компьютерные системы. Программная реализация функций криптографической защиты информации. Аппаратная реализация функций криптографической защиты информации. Устройства криптографической защиты данных: программно-аппаратный комплекс «Аккорд», персональное средство криптографической защиты информации (ПСКЗИ) ШИПКА.

2.4. Обеспечение конфиденциальности информации в IP-сетях

Основы построения IP-сетей и обеспечения безопасности информации в них. Особенности протокола TCP/IP. Виртуальные частные сети (VPN). Протоколы PPTP и L2TP. Анализ возможных уязвимостей протокола PPTP в реализации Micrsoft. Протоколы SSL и TLS. Протоколы IPSEC и распределение ключей. Протоколы IPSec и трансляция сетевых адресов. Обзор программно-аппаратного комплекса ViPNet CUSTOM.

3. Обеспечение доступности информации применением средств программно-аппаратной защиты

3.1. Обеспечение доступности информации средствами операционной системы

Управление правами доступа к ресурсам в операционных системах семейства MS Windows. Учетные записи пользователей и групп. Управление доступом и глобальными параметрами. Основные сведения об учетных записях групп. Оснастка "Локальные пользователи и группы"

3.2. Обработка информации на рабочих станциях и обеспечение ее доступности

Блокирование рабочей станции на аппаратном уровне. Аппаратные средства доверенной загрузки. Основные концепции и реализация аутентификации. Этапы доверенной загрузки.

3.3. Обеспечение доступности информации в локальных сетях

Межсетевые экраны и их классификация. Определение типов межсетевых экранов. Межсетевые экраны прикладного уровня. Межсетевые экраны с пакетной фильтрацией. Гибридные межсетевые экраны. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана с использованием возможностей брандмауэра Windows.

4. Обеспечение целостности информации с помощью программных и аппаратных средств

4.1. Терминология резервирования. Оперативное и автономное резервирование. Типы резервирования. Виды RAID-массивов. Исходные типы RAID-массивов. RAID-контроллеры. Основы резервирования данных. Варианты резервирования данных

4.2. Обеспечение целостности при передаче информации по сетям

Защищенные протоколы. Протокол HTTPS. Безопасность при использовании технологии передачи данных Wi-Fi. Возможности прослушивания трафика администратором Wi-Fi. WPA/WEP.

5. Комплексные системы защиты информации

5.1. Обеспечение антивирусной защиты информационных систем

Обеспечение антивирусной защиты сетевой инфраструктуры на основе приложений компании «Лаборатория Касперского». Kaspersky® Administration Kit. Развертывание антивирусной защиты в сети предприятия.

5.2. Предотвращение утечек информации (DLP) и учет рабочего времени

Контроль служебной переписки в почте и мессенджерах (Outlook, Яндекс.Почта, Skype, Mail.Agent). Контроль съемных носителей информации. Перехват ввода с клавиатуры. Фиксация всех файловых операций (чтение, запись, редактирование, копирование), процессов запуска и установки ПО. Учет рабочего времени, включая мониторинг активности в приложениях..

5.3. Системы обнаружения и предотвращения вторжений

Архитектура и технология IDS. Виды IDS по месту установки. Сетевые системы обнаружения вторжения (NIDS). Хостовая система обнаружения вторжений (HIDS).

6. Основы веб-безопасности

6.1. Цели атаки на веб-ресурсы предприятия

Основные цели, преследуемые злоумышленником в процессе атаки. Похищение информации, модификация информации, нарушение доступности информационного ресурса.

6.2. Методы и инструменты злоумышленника для атаки на веб-ресурсы

Прослушивание сети (sniffing), ARP spoofing, Сканирование. Генерация пакетов. Троянские программы. Эксплойты.

6.3. Классификация сетевых атак.

Классификация по типу атаки. Классификация по местоположению злоумышленника и атакуемого объекта. Классификация по уровню модели OSIАтаки типа spoofing.

3.3. Темы практических занятий

1. Анализ рынка биометрических систем доступа к АРМ;
2. Обеспечение доступности информации программно-аппаратными средствами защиты;
3. Общие принципы парольной защиты документов;
4. Персональные средства криптографической защиты информации;
5. Обеспечение целостности информации программно-аппаратными средствами защиты;
6. Автоматизированные системы в защищенном исполнении;
7. Конфиденциальность информации в IP-сетях;
8. Механизмы обеспечения конфиденциальности на уровне ОС;
9. Полностью контролируемые компьютерные системы;
10. Проведение расследования инцидентов ИБ.

3.4. Темы лабораторных работ

1. Лабораторная работа № 7: Системы анализа защищенности корпоративной сети и ОС на примере программы XSpider;
2. Лабораторная работа № 10: Анализ уязвимостей веб-сайтов на примере сайта базовой кафедры МЭИ;
3. Лабораторная работа № 8: Анализ трафика сети на наличие чувствительных к краже данных;
4. Лабораторная работа № 6. Корпоративная антивирусная защита;
5. Лабораторная работа №1: Анализ уязвимостей доступа к ОС Microsoft Windows;
6. Лабораторная работа № 4: «Использование программно-аппаратного комплекса «Аккорд»;
7. Лабораторная работа № 3. «Изучение биометрического комплекса (ПО BioLink Authentication Center и сканер Biolink U-Match)»;
8. Лабораторная работа №2: Логический вход в ОС Microsoft Windows с помощью аппаратных ключей;
9. Лабораторная работа № 5: Средство криптографической защиты информации CryptoPro;
10. Лабораторная работа № 9: Атака на сетевое оборудование с целью отказа в обслуживании.

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Введение"

2. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений"
3. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Обеспечение доступности информации применением средств программно-аппаратной защиты"
4. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Обеспечение целостности информации с помощью программных и аппаратных средств"
5. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Комплексные системы защиты информации"

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации проводятся по разделу "Введение"
2. Консультации проводятся по разделу "Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений"
3. Консультации проводятся по разделу "Обеспечение доступности информации применением средств программно-аппаратной защиты"
4. Консультации проводятся по разделу "Обеспечение целостности информации с помощью программных и аппаратных средств"
5. Консультации проводятся по разделу "Комплексные системы защиты информации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Введение"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Обеспечение доступности информации применением средств программно-аппаратной защиты"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Обеспечение целостности информации с помощью программных и аппаратных средств"
5. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Комплексные системы защиты информации"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)						Оценочное средство (тип и наименование)
		1	2	3	4	5	6	
Знать:								
Способы обнаружения и идентификации инцидентов информационной безопасности в процессе эксплуатации автоматизированной системы	ИД-1$_{ОПК-1.3}$	+						Контрольная работа/Контрольное мероприятие № 1 Контрольная работа/Контрольное мероприятие № 5
Типовые программные и программно-аппаратные средства резервирования и восстановления информации в автоматизированных системах	ИД-1$_{ОПК-1.3}$				+			Контрольная работа/Контрольное мероприятие № 2 Контрольная работа/Контрольное мероприятие № 6
Способы осуществления диагностики и мониторинга систем защиты автоматизированных систем	ИД-1$_{ОПК-1.4}$					+	+	Контрольная работа/Контрольное мероприятие № 4 Контрольная работа/Контрольное мероприятие № 8
Особенности проведения работ по установке, настройке, администрированию, обслуживанию и проверке работоспособности программно-аппаратных и технических средств защиты информации в автоматизированных системах	ИД-1$_{ОПК-1.4}$		+	+				Контрольная работа/Контрольное мероприятие № 3 Контрольная работа/Контрольное мероприятие № 7
Уметь:								

Администрировать системы обнаружения и идентификации инцидентов информационной безопасности в процессе эксплуатации автоматизированной системы	ИД-1$_{ОПК-1.3}$	+						Контрольная работа/Контрольное мероприятие № 1 Контрольная работа/Контрольное мероприятие № 5
Проводить установку и настройку программных и программно-аппаратных средства резервирования и восстановления информации в автоматизированных системах	ИД-1$_{ОПК-1.3}$				+			Контрольная работа/Контрольное мероприятие № 2 Контрольная работа/Контрольное мероприятие № 6
Выполнять оценку защищенности информации, идентификацию и ликвидацию инцидентов информационной безопасности в процессе эксплуатации автоматизированных систем	ИД-1$_{ОПК-1.4}$		+	+				Контрольная работа/Контрольное мероприятие № 3 Контрольная работа/Контрольное мероприятие № 7
Применять типовые программно-аппаратные средства защиты информации в автоматизированных системах и базах данных	ИД-1$_{ОПК-1.4}$					+	+	Контрольная работа/Контрольное мероприятие № 4 Контрольная работа/Контрольное мероприятие № 8

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

5 семестр

Форма реализации: Письменная работа

1. Контрольное мероприятие № 1 (Контрольная работа)
2. Контрольное мероприятие № 3 (Контрольная работа)
3. Контрольное мероприятие № 5 (Контрольная работа)
4. Контрольное мероприятие № 7 (Контрольная работа)

6 семестр

Форма реализации: Письменная работа

1. Контрольное мероприятие № 2 (Контрольная работа)
2. Контрольное мероприятие № 4 (Контрольная работа)
3. Контрольное мероприятие № 6 (Контрольная работа)
4. Контрольное мероприятие № 8 (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №5)

Экзамен (Семестр №6)

Для оценки используется только результаты промежуточной аттестации и экзамена

В диплом выставляется оценка за 6 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Борисов, М. А. Основы программно-аппаратной защиты информации : учебное пособие для вузов по направлениям ВПО "Прикладная математика и информатика", "Фундаментальная информатика и информационные технологии" / М. А. Борисов, И. В. Заводцев, И. В. Чижов . – 4-е изд., перераб. и доп . – М. : Эдиториал УРСС, 2016 . – 416 с. – (Основы защиты информации) . - ISBN 978-5-9710-2586-3 .;
2. Защита программ и данных : Программно-аппаратные средства обеспечения информационной безопасности : Учебное пособие для вузов по специальностям "Защищенные телекоммуникационные системы","Организация и технология защиты информации","Комплексное обеспечение информационной безопасности автоматизированных систем" / П. Ю. Белкин, и др. – М. : Радио и связь, 2000 . – 168 с. - ISBN 5-256-01533-8 : 50.00 .;
3. Платонов, В. В. Программно-аппаратные средства защиты информации : учебник для вузов по направлению "Информационная безопасность" по программам подготовки бакалавров, магистров, специалистов / В. В. Платонов, М. А. Полтавцева . – Москва :

Академия, 2020 . – 288 с. – (Высшее профессиональное образование . Бакалавриат) . - ISBN 978-5-4468-9702-5 .;
4. Душкин А. В., Барсуков О. М., Кравцов Е. В., Славнов К. В.- "Программно-аппаратные средства обеспечения информационной безопасности", Издательство: "Горячая линия-Телеком", Москва, 2018 - (248 с.)
https://e.lanbook.com/book/111053;
5. Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков- "Программно-аппаратные средства защиты информационных систем", Издательство: "Тамбовский государственный технический университет (ТГТУ)", Тамбов, 2017 - (194 с.)
https://biblioclub.ru/index.php?page=book&id=499013.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
7. **Журнал Science** - https://www.sciencemag.org/
8. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
9. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
10. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
11. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
Учебные аудитории для проведения	М-503, Учебная лаборатория	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная

лабораторных занятий	"Программно-аппаратная средства защиты информации"	сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

(название дисциплины)

5 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Контрольное мероприятие № 1 (Контрольная работа)
КМ-2 Контрольное мероприятие № 5 (Контрольная работа)
КМ-3 Контрольное мероприятие № 3 (Контрольная работа)
КМ-4 Контрольное мероприятие № 7 (Контрольная работа)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Введение					
1.1	Концептуальные основы информационной безопасности		+	+		
1.2	Основные понятия программно-аппаратной защиты информации		+	+		
2	Обеспечение доступности информации применением средств программно-аппаратной защиты					
2.1	Обеспечение доступности информации средствами операционной системы Управление правами доступа к ресурсам в операционных системах семейства MS Windows. Учетные записи пользователей и групп. Управление доступом и глобальными параметрами. Основные сведения об учетных записях групп. Оснастка "Локальные пользователи и группы"				+	+
2.2	Обработка информации на рабочих станциях и обеспечение ее доступности				+	+
2.3	Обеспечение доступности информации в локальных сетях				+	+
3	Обеспечение целостности информации с помощью программных и аппаратных средств					
3.1	Терминология резервирования. Оперативное и автономное резервирование. Типы резервирования. Виды RAID-массивов. Исходные типы RAID-массивов. RAID-контроллеры. Основы резервирования данных. Варианты резервирования данных				+	+
3.2	Обеспечение целостности при передаче информации по сетям				+	+
		Вес КМ, %:	25	25	25	25

6 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:
КМ-1 Контрольное мероприятие № 2 (Контрольная работа)
КМ-2 Контрольное мероприятие № 6 (Контрольная работа)
КМ-3 Контрольное мероприятие № 4 (Контрольная работа)
КМ-4 Контрольное мероприятие № 8 (Контрольная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Обеспечение конфиденциальности доступа к информации средствами операционных систем и пользовательских приложений					
1.1	Механизмы обеспечения конфиденциальности доступа к информации на уровне операционных систем		+	+		
1.2	Механизмы обеспечения конфиденциальности доступа к информации на уровне приложений		+	+		
1.3	Программно-аппаратные средства криптографической защиты информации		+	+		
1.4	Обеспечение конфиденциальности информации в IP-сетях		+	+		
2	Комплексные системы защиты информации					
2.1	Обеспечение антивирусной защиты информационных систем				+	+
2.2	Предотвращение утечек информации (DLP) и учет рабочего времени				+	+
2.3	Системы обнаружения и предотвращения вторжений				+	+
3	Основы веб-безопасности					
3.1	Цели атаки на веб-ресурсы предприятия				+	+
3.2	Методы и инструменты злоумышленника для атаки на веб-ресурсы				+	+
3.3	Классификация сетевых атак.				+	+
		Вес КМ, %:	25	25	25	25