Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 04.10.2023 10:50:47
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Программно-аппаратные средства защиты информации»

Направление подготовки

09.03.01 «Информатика и вычислительная техника»

Профиль
«Кибербезопасность автоматизированных систем»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

доцент, к.п.н., доцент  Д.Ф. Амиров

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 5
3 Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 10
3.4 Тематика семинарских/практических и лабораторных занятий 11
3.5 Тематика курсовых проектов (курсовых работ) 12
4 Учебно-методическое и информационное обеспечение 12
4.1 Нормативные документы и ГОСТы 12
4.2 Основная литература 12
4.3 Дополнительная литература 12
4.4 Электронные образовательные ресурсы 13
4.5 Лицензионное и свободно распространяемое программное обеспечение 13
4.6 Современные профессиональные базы данных и информационные справочные системы 13
5 Материально-техническое обеспечение 13
6 Методические рекомендации 13
6.1 Методические рекомендации для преподавателя по организации обучения 13
6.2 Методические указания для обучающихся по освоению дисциплины 14
7 Фонд оценочных средств 14
7.1 Методы контроля и оценивания результатов обучения 14
7.2 Шкала и критерии оценивания результатов обучения 14
7.3 Оценочные средства 15

1 Цели, задачи и планируемые результаты обучения по дисциплине

К основным целям освоения дисциплины «Программно-аппаратные средства защиты информации» следует отнести:

- ознакомление студентов с современными программно-аппаратными средствами защиты информации в компьютерных системах;
- овладение методами решения задач программно-аппаратной защиты информации.

К основным задачам освоения дисциплины «Программно-аппаратные средства защиты информации» следует отнести:

- обучение студентов современным методам программно-аппаратной защиты информации;
- приобретение профессиональной компетентности в программно-аппаратных средствах защиты информации;
- умение ориентироваться в продуктах и тенденциях развития средств программно-аппаратной защиты информационных технологий.

Обучение по дисциплине «Программно-аппаратные средства защиты информации» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	**Индикаторы достижения компетенции**
ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программноаппаратных средств администрируемой сети; Классификация ОС согласно классам безопасности; Средства защиты от несанкционированного доступа ОС и СУБД; ИПК-2.2. Уметь: Применять аппаратные и программные средства защиты сетевых устройств от несанкционированно го доступа Настраивать параметры и сегментировать элементы администрируемой сети ИПК-2.3. Владеет: Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированно го доступа Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированно го доступа Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов) Документирование настроек средств обеспечения безопасности удаленного

2 Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации » относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.1) основной образовательной программы бакалавриата (Б1.1.42).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Основы ИКТ», «Криптографические методы защиты информации».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. 144 академических часов (лекции – 4 часа, лабораторные занятия – 68 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 7 семестре.

Структура и содержание дисциплины «Программно-аппаратные средства защиты информации» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	7	1-18
	В том числе:			
1.1	Лекции	4	7	1-2
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	68	7	3-18
2	**Самостоятельная работа**	**72**		
	В том числе:			
2.1	СРС	72	7	1-18
3	**Промежуточная аттестация**	**-**	7	6-17
	Зачет/диф.зачет/экзамен		7	По расписанию
	Итого	**144**		

3.2 Тематический план изучения дисциплины
(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Самостоятельная работа						

1.1	Разработка политики информационной безопасности. Методология политики безопасности компьютерных систем. Основные положения политики информационной безопасности. Жизненный цикл политики безопасности. Принципы политики безопасности.	4					4
1.2	Разработка политики информационной безопасности компьютерной системы.	4					4
1.3	Разработка модели угроз компьютерной системы.						
1.4	Объекты угроз. Классификация угроз по способу их осуществления. Классификация объектов угроз. Функциональная модель системы защиты. Состав и назначение функциональных блоков. Основные группы механизмов защиты. Функциональная модель. Рекомендации по отдельным уровням функциональной модели.	4					4
1.5	Дискреционные и мандатные модели.	4					4
1.6	Система защиты информации от несанкционированного доступа «СТРАЖ NT». Установка и снятие СЗИ. Замкнутая программная среда.	4					4
1.7	Система защиты информации от несанкционированного доступа «СТРАЖ NT». Управление пользователями. Учет носителей и контроль устройств.	4					4
1.8	Понятие доступа и монитора безопасности. Обеспечение гарантий выполнения политики безопасности. Методология проектирования гарантированно защищенных КС. Метод генерации изолированной программной среды.	4					4
1.9	Дискреционные модели. Модель АДЕПТ-50. Пятимерное пространство безопасности Хартстона. Мандатная модель. Модель Белла-Лападула. Первое правило модели Белла-Лападула. Второе правило модели Белла-Лападула. Описание модели.	4					4
1.10	Идентификация и аутентификация. Основные понятия и классификация. Простая	4					4

	аутентификация. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе сертификатов. Биометрическая идентификация и аутентификация пользователей.						
1.11	Строгая аутентификация. Протоколы аутентификации с симметричными алгоритмами шифрования. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций. Аутентификация с использованием асимметричных алгоритмов шифрования. Аутентификация, основанная на использовании цифровой подписи. Протоколы аутентификации с нулевой передачей значений. Упрощенная схема аутентификации с нулевой передачей знаний. Параллельная схема аутентификации с нулевой передачей знаний.	4					4
1.12	Протокол идентификации и аутентификации в ОС Windows	4					4
1.13	Протокол идентификации и аутентификации в ОС Windows . Протокол аутентификации Kerberos. Сохранность паролей учетных записей. Windows. Защита паролей. Кража SAM-файла. Захват привилегий. Сброс пароля. Взлом вторичных паролей. Система разграничения доступа ОС LINUX. Возможности стандартной системы разграничения доступа ОС Linux. Недостатки стандартной системы разграничения доступа ОС Linux. Возможности наиболее известных средств совершенствования разграничения доступа ОС Linux.	4					4
1.14	Протокол аутентификации Kerberos.	4					4
1.15	Система разграничения доступа ОС LINUX.	4					4
1.16	Защита файловой системы Windows. Разрешения для файлов и папок. Шифрующая файловая система (EFS) Encrypting File System. Технология шифрования. Восстановление данных. Процесс	4					4

	шифрования. Процесс дешифрирования. Процесс восстановления. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing). Типовые задачи администрирования. Администрирование дисков в Windows. Сходства и различия между Disk Management и Disk Administrator.						
1.17	Шифрующая файловая система (EFS) Encrypting File System.	4					4
1.18	Защита файловой системы OS Linux. Файловая система OS Linux . Основные концепции файловой системы. Виртуальная Файловая Система (VFS). Файловые системы EXT2 (The Second Extended File System).	4					4
2	**Лабораторные работы**						
2.1	Установка программного комплекса ViPNet Administrator 4.x.Создание структуры защищенной сети	2			2		
2.2	Настройка резервного копирования данных и восстановление данных в ПО ViPNet Administrator. Развертывание рабочего места помощника главного администратора.	4			4		
2.3	Модификация защищенной сети. Компрометация.	4			4		
2.4	Настройка политик безопасности в ViPNet PolicyManager. Установка ViPNet Coordinator в качестве межсетевого шлюза	4			4		
2.5	Первоначальная настройка межсетевого взаимодействия. Модификация межсетевого взаимодействия.	4			4		
2.6	Настройка локальных и транзитных фильтров открытой сети. Настройка фильтров защищенной сети.	4			4		
2.7	Настройка трансляции адресов (NAT). Туннелирование в ViPNet Coordinator.	4			4		
2.8	ViPNetClient 4 – VPN и персональный сетевой экран. Криптопровайдер ViPNetCSP.	4			4		
2.9	Работа с приложениями	4			4		

2.10	Установка и инициализация комплекса «Соболь». Настройка общих параметров.	2			2		
2.11	Настройка и эксплуатация комплекса «Соболь».	4			4		
2.12	Установка и инициализация комплекса «Secret Net 5.0-C». Настройка общих параметров.	4			4		
2.13	Управление режимами входа в систему. Управление персональными идентификаторами пользователей.	4			4		
2.14	Управление устройствами в Secret Net 5.0.	4			4		
2.15	Полномочное разграничение доступа в Secret Net 5.0.	4			4		
2.16	Контроль целостности и замкнутая программная среда в Secret Net 5.0	4			4		
2.17	Шифрование файлов в Secret Net 5.0.	4			4		
3	**Лекции**						
3.1	Принцип функционирования защищенной сети ViPNet. Архитектура ViPNet Administrator 4.x. Модификация защищенной сети и настройка политик безопасности на узлах. Модификация защищенной сети и настройка политик безопасности на узлах.	2	2				
3.2	Работа с ViPNet Coordinator for Windows. ViPNetClient.	2	2				
	Итого	**144**	**4**		**68**		**72**

3.3 Содержание дисциплины

Тема1. Понятие политики безопасности при программно-аппаратной защите информации.

Разработка политики информационной безопасности. Методология политики безопасности компьютерных систем. Основные положения политики информационной безопасности. Жизненный цикл политики безопасности. Принципы политики безопасности.

Тема 2. Архитектура системы программно-аппаратной защиты.

Объекты угроз. Классификация угроз по способу их осуществления. Классификация объектов угроз. Функциональная модель системы защиты. Состав и назначение функциональных блоков. Основные группы механизмов защиты. Функциональная модель. Рекомендации по отдельным уровням функциональной модели.

Тема 3. Модель компьютерной системы.

Понятие доступа и монитора безопасности. Обеспечение гарантий выполнения политики безопасности. Методология проектирования гарантированно защищенных КС. Метод генерации изолированной программной среды.

Тема 4. Модели типовых политик безопасности компьютерных средств защиты информации.

Дискреционные модели. Модель АДЕПТ-50. Пятимерное пространство безопасности Хартстона. Мандатная модель. Модель Белла-Лападула. Первое правило модели Белла-Лападула. Второе правило модели Белла-Лападула. Описание модели.

Тема 5. Программно-аппаратные средства идентификации и аутентификации пользователей.

Идентификация и аутентификация. Основные понятия и классификация. Простая аутентификация. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе сертификатов. Биометрическая идентификация и аутентификация пользователей.

Строгая аутентификация. Протоколы аутентификации с симметричными алгоритмами шифрования. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций. Аутентификация с использованием асимметричных алгоритмов шифрования. Аутентификация, основанная на использовании цифровой подписи. Протоколы аутентификации с нулевой передачей значений. Упрощенная схема аутентификации с нулевой передачей знаний. Параллельная схема аутентификации с нулевой передачей знаний. Инфраструктура открытых ключей.

Тема 6. Механизм идентификации и аутентификации в ОС. Разграничение доступа.

Протокол идентификации и аутентификации в ОС Windows . Протокол аутентификации Kerberos. Сохранность паролей учетных записей. Windows. Защита паролей. Кража SAM-файла. Захват привилегий. Сброс пароля. Взлом вторичных паролей. Система разграничения доступа ОС LINUX. Возможности стандартной системы разграничения доступа ОС Linux. Недостатки стандартной системы разграничения доступа ОС Linux. Возможности наиболее известных средств совершенствования разграничения доступа ОС Linux.

Тема 7. Защита файловой системы в ОС.

Защита файловой системы Windows. Разрешения для файлов и папок. Шифрующая файловая система (EFS) Encrypting File System. Технология шифрования. Восстановление данных. Процесс шифрования. Процесс дешифрирования. Процесс восстановления. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing). Типовые задачи администрирования. Администрирование дисков в Windows. Сходства и различия между Disk Management и Disk Administrator. Защита файловой системы OS Linux. Файловая система OS Linux. Основные концепции файловой системы. Виртуальная Файловая Система (VFS). Файловые системы EXT2 (The Second Extended File System).

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1. Лабораторные занятия

Лабораторная работа 1. Установка программного комплекса ViPNet Administrator 4.x.Создание структуры защищенной сети.

Лабораторная работа 2. Настройка резервного копирования данных и восстановление данных в ПО ViPNet Administrator. Развертывание рабочего места помощника главного администратора.

Лабораторная работа 3. Модификация защищенной сети. Компрометация.

Лабораторная работа 4. Настройка политик безопасности в ViPNet PolicyManager. Установка ViPNet Coordinator в качестве межсетевого шлюза

Лабораторная работа 5. Первоначальная настройка межсетевого взаимодействия. Модификация межсетевого взаимодействия.

Лабораторная работа 6. Настройка локальных и транзитных фильтров открытой сети. Настройка фильтров защищенной сети.

Лабораторная работа 7. Настройка трансляции адресов (NAT). Туннелирование в ViPNet Coordinator.

Лабораторная работа 8. ViPNetClient 4 – VPN и персональный сетевой экран. Криптопровайдер ViPNetCSP.

Лабораторная работа 9. Работа с приложениями

Лабораторная работа 10. Установка и инициализация комплекса «Соболь». Настройка общих параметров.

Лабораторная работа 11. Настройка и эксплуатация комплекса «Соболь».

Лабораторная работа 12. Установка и инициализация комплекса «Secret Net 5.0-C». Настройка общих параметров.

Лабораторная работа 13. Управление режимами входа в систему. Управление персональными идентификаторами пользователей.

Лабораторная работа 14. Управление устройствами в Secret Net 5.0.

Лабораторная работа 15. Полномочное разграничение доступа в Secret Net 5.0.

Лабораторная работа 16. Контроль целостности и замкнутая программная среда в Secret Net 5.0

Лабораторная работа 17. Шифрование файлов в Secret Net 5.0.

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом не запланировано.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность».

Профессиональные стандарты:

06.032 Специалист по безопасности компьютерных систем и сетей. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 533н;

06.033 Специалист по защите информации в автоматизированных системах. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 г. № 525н).

4.2 Основная литература

1) Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д.В. Маршаков, Д.В. Фатхи ; Донской государственный технический университет. Ростов-на-Дону: ДГТУ, 2021. - 228 с. - ISBN 978-5-7890-1878-1 — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://reader.lanbook.com/book/237770. — Режим доступа: для авториз. пользователей.

2) Булычёв, Г. Г. Программно-аппаратные средства защиты информации : учебно-методическое пособие / Г. Г. Булычёв. — Москва : РТУ МИРЭА, 2022 — Часть 1 — 2022. — ISBN 978-5-7339-1652-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310781. — Режим доступа: для авториз. пользователей.

3) Булычёв, Г. Г. Программно-аппаратные средства защиты информации : учебно-методическое пособие / Г. Г. Булычёв. — Москва : РТУ МИРЭА, 2022 — Часть 2 — 2022. — ISBN 978-5-7339-1653-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310784. — Режим доступа: для авториз. пользователей.

4.3 Дополнительная литература

1) Горлов, А.П. Автоматизированная система оценки эффективности программно-аппаратных средств защиты информации / А.П. Горлов, М.Ю. Рытов, Д.А. Лысов // Автоматизация и моделирование в проектировании и управлении . — 2019. — № 2. — С. 25-32. — ISSN 2658-6436. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/311268 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей..

2) Жмуров, Д. Б. Программно-аппаратные средства защиты информации : учебное пособие / Д. Б. Жмуров, С. В. Жуков. — Самара : Самарский университет, 2022. — ISBN 978-5-7883-1799-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/336515 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей.

3) Бутин, А. А. Программно-аппаратные средства защиты информации : учебное пособие / А. А. Бутин, Н. И. Глухов, С. И. Носков. — 2-е изд., перераб. и доп. — Иркутск : ИрГУПС, 2022. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/342113 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей.

4.4 Электронные образовательные ресурсы

1. Федоров Н.В. . Программно-аппаратные средства защиты информации. Электронный образовательный ресурс. Московский Политех, 2020- https://lms.mospolytech.ru/course/view.php?id=495
2. Secret Net Studio https://www.securitycode.ru/products/secret-net-studio/
3. Infotecs https://infotecs.ru/products/filter/type-is-33/apply/

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. ПО «ViPNet Administrator 4»

2. Электронный замок "Соболь".
3. Система защиты "Secret Net Studio".
4. ПАК защищенного хранения информации «Секрет Особого Назначения»
5. Комплекс средств защиты информации от НСД «Аккорд–АМДЗ»
6. ПАК защиты информации от несанкционированного доступа «АККОРД-Win64» (версия 5.0).

4.6 Современные профессиональные базы данных и информационные справочные системы

Локальный научно-образовательный комплекс по дисциплине "Программно-аппаратная защита информации".

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической и практической подготовки студентов являются лекции и лабораторные работы.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

Показатель	Критерии оценивания			
	2	**3**	**4**	**5**
ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения				
ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Классификация ОС согласно классам безопасности; Средства защиты от несанкционированного доступа ОС и СУБД; ИПК-2.2. Уметь: Применять аппаратные и программные средства	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенным и знаниями.

защиты сетевых устройств от несанкционированного доступа Настраивать параметры и сегментировать элементы администрируемой сети ИПК-2.3. Владеет: Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа Настройка средств обеспечения безопасности удаленного доступа (операционной системы и				

специализированных протоколов) Документирование настроек средств обеспечения безопасности удаленного				

Форма промежуточной аттестации: экзамен.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.

Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

Оценочные средства для текущей аттестации

Компьютерное тестирование.

Оценочные средства для промежуточной аттестации

Экзамен.

Список вопросов для экзамена по дисциплине

1. Компьютерная система как объект защиты информации
2. Понятие угрозы информационной безопасности в КС
3. Классификация и общий анализ угроз информационной безопасности в КС
4. Случайные угрозы информационной безопасности КС
5. Преднамеренные угрозы информационной безопасности КС
6. Разработка политики информационной безопасности КС
7. Методология политики безопасности компьютерных систем
8. Основные положения политики информационной безопасности КС
9. Жизненный цикл политики безопасности КС
10. Функциональная модель системы защиты. Состав и назначение функциональных блоков
11. Понятие доступа и монитора безопасности
12. Методология проектирования гарантированно защищенных КС
13. Метод генерации изолированной программной среды
14. Модель АДЕПТ-50
15. Пятимерное пространство безопасности Хартстона
16. Мандатная модель доступа
17. Модель Белла-Лападула
18. Идентификация и аутентификация. Основные понятия и классификация
19. Простая аутентификация
20. Электронный замок "Соболь"
21. Биометрическая идентификация и аутентификация пользователей
22. Строгая аутентификация
23. Протоколы аутентификации с симметричными алгоритмами шифрования
24. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций
25. Аутентификация с использованием асимметричных алгоритмов шифрования
26. Аутентификация, основанная на использовании цифровой подписи
27. Протоколы аутентификации с нулевой передачей значений

28. Упрощенная схема аутентификации с нулевой передачей знаний
29. Параллельная схема аутентификации с нулевой передачей знаний
30. Протокол аутентификации Kerberos
31. Протокол идентификации и аутентификации в ОС Windows
32. Сохранность паролей учетных записей
33. Защита информации в файловой системе NTFS
34. Шифрующая файловая система (EFS) Encrypting File System
35. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing)
36. Администрирование дисков в Windows
37. Windows : Защита паролей
38. Возможности стандартной системы разграничения доступа ОС Linux
39. Система LIDS
40. Формат сертификатов открытых ключей X.509
41. Инфраструктура открытых ключей
42. Теоретические принципы построения биометрических систем
43. Вектор параметров при анализе рукописного почерка
44. Защита на уровне расширений BIOS
45. Защита на уровне загрузчиков операционной системы
46. Сертификат открытых ключей X.509

Пример билета.

1. Компьютерное тестирование.
2. Аутентификация с использованием асимметричных алгоритмов шифрования.
3. Практическая настройка программно-аппаратных средств защиты.