МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФИЗИКО- МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

УТВЕРЖДАЮ
Проректор по УР и КО
_____ С.А. Льянова
«29» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.05.01 Методы и средства защиты информации

Основной профессиональной образовательной программы
академического бакалавриата

09.03.02 «Информационные системы и технологии»

Квалификация выпускника

Академический бакалавр

Форма обучения

Очная

Магас, 2023

1. Цели и задачи освоения дисциплины «Методы и средства защиты информации»

Целями освоения дисциплины Б1.В.ДВ.05.01 «Методы и средства защиты информации» являются формирование у студентов компетенций в области информационной безопасности и применения на практике методов и средств защиты информации.

Формируемые дисциплиной знания и умения готовят выпускника данной образовательной программы к выполнению следующих обобщенных трудовых функций (трудовых функций):

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	Наименование	Уровень квалификации	Наименование	Код	Уровень (подуровень) квалификации
06.011 Администратор баз данных	D	Обеспечение информационной безопасности на уровне БД	6	Разработка политики информационной безопасности на уровне БД	D/01.6	6
				Контроль соблюдения регламентов по обеспечению безопасности на уровне БД	D/02.6	6
				Оптимизация работы систем безопасности с целью уменьшения нагрузки на работу БД	D/03.6	6
				Разработка регламентов и аудит системы безопасности данных	D/04.6	6
				Подготовка отчетов о состоянии и эффективности системы безопасности на уровне БД	D/05.6	6
				Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным	D/06.6	6

2. Место учебной дисциплины в структуре основной профессиональной образовательной программы бакалавриата

Дисциплина «Методы и средства защиты информации» изучается в блоке Б1.В и является одной из дисциплин вариативной части, формируемой участниками образовательных отношений, и имеет соответствующий шифр Б1.В.ДВ.05.01 подготовки бакалавриата по направлению 09.03.02 «Информационные системы и технологии».

Дисциплины и практики, знания и умения, по которым необходимы как "входные" при изучении данной дисциплины	Безопасность жизнедеятельности Информатика
Дисциплины, практики, ГИА, для которых изучение данной дисциплины необходимо как «предшествующее»	Администрирование в информационных системах Управление данными Защита интеллектуальной собственности Корпоративные информационные системы

Формы работы студентов - в ходе изучения дисциплины предусмотрены семинарские занятия, выполнение домашних работ. Самостоятельная работа студентов, предусмотренная учебным планом, выполняется в ходе семестра в форме выполнения домашних заданий. Отдельные темы теоретического курса прорабатываются студентами самостоятельно в соответствии с планом самостоятельной работы и конкретными заданиями преподавателя с учетом индивидуальных особенностей студентов. Виды текущего контроля - проверка домашних заданий, устный опрос, проверка контрольной работы. Форма итогового контроля: 3 курс, 5 семестр –экзамен.

3. Результаты освоения дисциплины «Методы и средства защиты информации»:

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Категория (группа) компетенций	**Код и наименование компетенции**	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**
УК-2	**УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих пра-**	УК-2.1.: понимает виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие про-	Знать: виды ресурсов ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность.

	вовых норм, имеющихся ресурсов и ограничений	фессиональную деятельность. УК-2.2.:проводит анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.	Уметь: проводить анали поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно правовую документацию в сфере профессиональной деятельности.
ПК-4	**ПК-4. Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности**	ПК-4.1: использует специальные знания по работе с установленной БД; общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных; основы управления учетными записями пользователей; ПК-4.2: выполняет регламентные процедуры по резервированию данных; выбирать способ действия из известных; контролировать оценивать и корректировать свои действия; выполнять регламентные процедуры по восстановлению и проверке корректности восстановленных данных; выбирать способ действия из известных; контролировать оценивать и корректировать свои действия; применять специальные процедуры управления правами доступа пользователей ПК-4.3: запускает процедуры резервного копирования; мониторинга выполнения процедуры резервного копирования; контроля завершения процедуры резервного копирования; запуска процедуры восстановления БД; мониторинга выполнения процедуры восстановления БД; кон-	Знать: специальные знания по работе с установленной БД; общие основы решении практических задач по восстановлению БД и проверке корректности восстановлены данных; специальные знаний по работе с установленной БД основы управления учетными записями пользователей; специальные знания по работам с установленной БД. , Уметь: выполнять регламентные процедуры п резервированию данных; выбирать способ действия и известных; контролировать оценивать и корректировать свои действия; выполнят , регламентные процедуры п восстановлению и проверки корректности восстановлены данных; выбирать способ действия из известных контролировать, оценивать корректировать свои действия применять специальные процедуры управления правами доступа пользователей; Владеть навыками: запуск процедуры резервного копирования; мониторинг выполнения процедуры резервного копирования; контроля завершения ; процедуры резервного копирования; запуска процедуры восстановления БД мониторинга выполнения процедуры восстанов-

		троля завершения процедуры восстановления БД; назначения прав доступа пользователей к БД изменения прав доступа пользователей к БД; контроля соблюдения прав доступа пользователей к БД.	ления БД контроля завершения процедуры восстановления БД назначения прав доступа пользователей к БД; изменений прав доступа пользователей к БД
ПК-8	**ПК-8. Способность выполнять работы по разработке компонентов системных программных продуктов: компилятор, загрузчиков, сборщиков, системных утилит, драйверов устройств, по созданию инструментальных средств программирования**	ПК-8.1.: понимает синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; методологии разработки программного обеспечения; методологии и технологии проектирования и использования баз данных; технологии программирования; особенности выбранной среды программирования и системы управления базами данных; компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними; ПК-8.2: применяет выбранные языки программирования для написания программного кода; использовать выбранную среду программирования и средства системы управления базами данных; использовать возможности имеющейся технической и/или программной архитектуры;	Знать: синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; методологии разработки программного обеспечения; методологии и технологии проектирования и использования баз данных; технологии программирования; особенности выбранной среды программирования и системы управления базами данных; компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними; Уметь: применять выбранные языки программирования для написания программного кода; использовать выбранную среду программирования и средства системы управления базами данных; использовать возможности имеющейся технической и/или программной архитектуры

4. Структура и содержание дисциплины «Методы и средства защиты информации»

4.1. Структура дисциплины «Методы и средства защиты информации»

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Наименование разделов и тем дисциплины (модуля)	семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*						
			Контактная работа					Самостоятельная работа										
			Всего	Лекции	Практические занятия	Лабораторные занятия	Др. виды контакт.работы	Всего	Курсовая работа(проект)	Подготовка к экзамену	Другие виды самостоятельной работы	Собеседование	Коллоквиум	Проверка тестов	Проверка контрольн. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект) лр.
1.	Тема 1. Понятие и сущность информационной безопасности и защиты	5	8	2		2		4			4							
2.	Тема 2.Основные угрозы информационной безопасности	5	8	2		2		4			4							
3.	Тема 3.Правовой уровень обеспечения информационной	5	8	2		2		4			4							
4.	Тема 4. Административный уровень обеспечения информационной безопасности	5	8	2		2		4			4							
5.	Тема 5. Программно-технический уровень обеспечения защиты информации	5	8	2		2		4			4							
6.	Тема 6. Процедурный уровень информационной безопасности	5	8	2		2		4			4							
7.	Тема 7. Система защиты информации	5	8	2		2		4			4							
8.	Тема 8. Обеспечение режима конфиденциальности при работе с защищаемой информацией	5	8	2		2		4			4							
9.	Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации	5	12	4		2		6			6							

10.	Тема 10. Ответственность за правонарушения информационной безопасности и защиты информации	5	10	2		2		6			6							
11.	Тема 11. Анализ угроз. Проблемы безопасности IP-сетей. Пути решения проблем защиты информации в сетях. Политика безопасности	5	12	2		2		8			8							
12.	Тема 12. Международные стандарты безопасности. Стандарты информационной безопасности в Интернете. Отечественные стандарты безопасности информационных технологий	5	12	2		2		8			8							
13.	Тема 13. Симметричные криптосистемы. Блочные шифры. Конструкция Фейстеля. Режимы шифрования блочных шифров. Стандарты блочного шифрования. Стандарт России - ГОСТ 28147-89. Поточные шифры. Шифр RC4.	5	13	4		2		7			7							
14.	Тема 14. Введение в теорию чисел. Метод распределения ключей Диффи-Хеллмана. Криптосистема RSA. Криптосистема ЭльГамаля. Стандарты России ГОСТ 34.10, ГОСТ 34.11	5	10	2		2		6			6							
15.	Тема 15. Простая аутентификация. Строгая аутентификация. Биометрическая аутентификация	5	10	2		2		6			6							
16.	Тема 16. Обеспечение безопасности ОС. Технологии межсетевых экранов.		10	2		2		6			6							
	Курсовая работа (проект)																	
	Подготовка к экзамену																	
	Общая трудоемкость, в часах		180	36		32		*85*			85							
	Промежуточная аттестация																	
	Форма																	
	Зачет																	
	Зачет с оценкой																	
	Экзамен		27															

4.2. Содержание дисциплины

№	Название темы	Содержание
1.	Понятие и сущность информационной безопасности и защиты информации	Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. Основные компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие понятия «информационная безопасность». Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации.
2.	Основные угрозы информационной безопасности	Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.
3.	Правовой уровень обеспечения информационной безопасности	Основные федеральные органы, генерирующие Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне. Степени конфиденциальности сведений, составляющих коммерческую тайну. Методика формирования на фирме перечня сведений, относящихся к коммерческой тайне.
4	Административный уровень обеспечения информационной безопасности	Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки политики ИБ. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ

5.	Программно- технический уровень обеспечения защиты информации	Программные сервисы защиты информации в ИС. Идентификация и аутентификация пользователей как передовой рубеж защиты информации. Базовые методы парольной аутентификации. Модели разграничения доступа к информации. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности. Базовые методы криптографического преобразования данных. Потоковое и блочное шифрование. Процедура формирования электронной подписи. Экранирование информации в информационнотелекоммуникационных сетях (ИТС). Основные сервисы защиты в ИТС. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.
6.	Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня Управление персоналом Физическая защита Поддержание работоспособности Реагирование на нарушения режима безопасности Планирование восстановительных работ.
7.	Система защиты информации	Процесс развития средств и методов защиты информации Этапы развития системы защиты информации в настоящее время Комплексный подход к построению системы защиты информации Системный подход к построению системы защиты информации Цели задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации. Структура систем защиты информации на современном этапе. Методы (виды) обеспечения защиты информации.
8.	Обеспечение режима конфиденциальности при работе с защищаемой информацией	Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Допуск должностных лиц, работников к конфиденциальной информации Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям
9.	Контроль за соблюдением требований информационной безопасности и защиты информации	Основные положения по осуществлению контроля, назначение, цель и задачи контроля. Основные мероприятия по осуществлению контроля. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа Проведение служебного расследования по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений режима конфиденциальности.

10.	Ответственность за правонарушения информационной безопасности и защиты информации	Понятие и виды юридической ответственности за нарушение правовых норм по защите информации Меры дисциплинарной ответственности согласно Трудового кодекса РФ Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности Уголовная ответственность за правонарушения в области защиты государственной тайны Уголовная ответственность за правонарушения в области конфиденциальной информации.
11.	Анализ угроз. Проблемы безопасности IP-сетей. Пути решения проблем защиты информации в сетях. Политика безопасности	Рост популярности Интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д. . В ближайшем будущем их число во много раз возрастет, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям также постоянно возрастает. На практике IP-сети уязвимы для многих способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется.
12.	Международные стандарты безопасности. Стандарты информационной безопасности в Интернете. Отечественные стандарты безопасности информационных технологий	В последнее время в мире бурно развивается электронная коммерция посредством сети Интернет. Развитие электронной коммерции в основном определяется прогрессом в области безопасности информации. При этом базовыми задачами являются обеспечение доступности, конфиденциальности, целостности и юридической значимости информации. По оценке Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень одной из международных проблем. Поэтому чрезвычайно важно добиваться эффективного решения проблем обеспечения безопасности коммерческой информации в глобальной сети Интернет и смежных intranet-сетях, которые по своей технической сущности не имеют принципиальных отличий и различаются в основном масштабами и открытостью.
13.	Симметричные криптосистемы. Блочные шифры. Конструкция Фейстеля. Режимы шифрования блочных шифров. Стандарты блочного шифрования. Стандарт России - ГОСТ 28147-89. Поточные шифры. Шифр RC4.	Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват. Обмен информацией осуществляется в 3 этапа: 1. отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар); 2. отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю; 3. получатель получает сообщение и расшифровывает

		его. Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.
14.	Введение в теорию чисел. Метод распределения ключей Диффи-Хеллмана. Криптосистема RSA. Криптосистема ЭльГамаля. Стандарты России ГОСТ 34.10, ГОСТ 34.11	Криптосистемы Диффи-Хеллмана и Эль-Гамаля основаны на вычислительной сложности задачи дискретного логарифмирования. Вычисление y=ax {mod p} (p – простое число или степень простого числа, 1<x<p-1, 1<a<p-1, 1<b<p-1, ac = b{mod p}) выполняется просто, но вычисление x = logay{mod p} выполняется достаточно сложно. Алгоритм Диффи-Хеллмана предназначен только для генерации ключа симметричного шифрования, который затем будет использован субъектами A и B для защищенного обмена сообщениями по открытой сети.
15.	Простая аутентификация. Строгая аутентификация. Биометрическая аутентификация	Процедура проверки подлинности. Она может быть односторонней или взаимной, обычно проводится с помощью криптографических способов. Не следует путать с авторизацией (процедурой предоставления субъекту определённых прав) и идентификацией (процедурой распознавания субъекта по его идентификатору
16.	Обеспечение безопасности ОС. Технологии межсетевых экранов.	Сетевые атаки несут с собой большую опасность для корпоративных сетей и домашних пользователей. Для их предотвращения, обнаружения и блокирования человечество придумало разнообразные механизмы и средства, их реализующие. Однако надо понимать, что невозможно рассмотреть все до единого механизмы и все аспекты, связанные с разнородными средствами защиты.

5. Образовательные технологии

В освоении дисциплины используются следующие образовательные технологии:

- Компьютерные классы с набором лицензионного базового программного обеспечения для проведения лабораторных занятий;
- Skype, ЭИОС на платформе Moodle для проведения дистанционного обучения и консультаций. Технология мультимедиа в режиме диалога.
- Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории). Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.

При подготовке бакалариатов используются основные формы проведения учебных занятий:

- интерактивные лекции;

- лекции-пресс-конференции;
- тренинги и семинары по развитию профессиональных навыков;
- практические (семинарские) занятия, групповые дискуссии и обмен мнениями, разбор альтернативных ситуаций;
- индивидуальные консультации;
- самостоятельная работа студентов с учебной литературой и первоисточниками, с интернет-ресурсами;
- экзамен.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых вовремя аудиторной работы. Вовремя самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301).

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного бюджетного образовательного учреждения высшего образования «Ингушский государственный университет» приказ от 30.10.2018 №807

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Тема 1. Понятие и сущность информационной безопасности и защиты информации	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	2
2	Тема 2. Основные угрозы информационной безопасности	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	2
3	Тема 3.Правовой уровень обеспечения информационной безопасности	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	2
4	Тема 4. Административный уровень обеспечения информационной безопасности	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	8
5	Тема 5. Программно-технический уровень обеспечения защиты информации	Тест	Подготовиться к тесту, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	8
6	Тема 6. Процедурный уровень информационной безопасности	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
7	Тема 7. Система защиты информации	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4

8	Тема 8. Обеспечение режима конфиденциальности при работе с защищаемой информацией	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	10
9	Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
10	Тема 10. Ответственность за правонарушения информационной безопасности и защиты информации	Тест	Подготовиться к тесту, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4
11	Анализ угроз. Проблемы безопасности IP-сетей. Пути решения проблем защиты информации в сетях. Политика безопасности	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	2
12	Международные стандарты безопасности. Стандарты информационной безопасности в Интернете. Отечественные стандарты безопасности информационных технологий	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	2
13	Симметричные криптосистемы. Блочные шифры. Конструкция Фейстеля. Режимы шифрования блочных шифров. Стандарты блочного шифрования. Стандарт России - ГОСТ 28147-89. Поточные шифры. Шифр RC4.	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	2

14	Введение в теорию чисел. Метод распределения ключей Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля. Стандарты России ГОСТ 34.10, ГОСТ 34.11	Тест	Подготовиться к тесту, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	10
15	Простая аутентификация. Строгая аутентификация. Биометрическая аутентификация	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	10
16	Обеспечение безопасности ОС. Технологии межсетевых экранов.	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	7.1.1. -7.1.3.(ол) 7.1.4-7.1.6.(дл) Интернет- ресурсы	4

6.2. Методические указания по организации самостоятельной работы студентов

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, практические занятия, самостоятельную работу студента, консультации.

a. При изучении тем студентам необходимо повторить лекционный учебный материал, изучить рекомендованную литературу, а также учебный материал, находящийся в указанных информационных ресурсах.

На завершающем этапе изучения каждого модуля необходимо, воспользовавшись предложенными вопросами для самоконтроля, размещенными в электронной информационной образовательной среде (ЭИОС), проверить качество усвоения учебного материала.

В случае затруднения в ответах на поставленные вопросы рекомендуется повторить учебный материал.

b. После изучения каждого модуля дисциплины необходимо ответить на вопросы контрольного теста по данному модулю с целью оценивания знаний и получения баллов.

c. После изучения всех модулей приступить к выполнению кон-

трольной работы, руководствуясь методическими рекомендациями по ее выполнению.

d. По завершению изучения учебной дисциплины в семестре студент обязан пройти промежуточную аттестацию. Вид промежуточной аттестации определяется рабочим учебным планом. Форма проведения промежуточной аттестации - компьютерное тестирование с использованием автоматизированной системы тестирования знаний студентов в ЭИОС.

e. К промежуточной аттестации допускаются студенты, выполнившие требования рабочего учебного плана.

6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций при изучении учебной дисциплины в процессе освоения образовательной программы

Типовой вариант задания на контрольную работу

№ п/п	Наименование тем
1	Понятие и сущность информационной безопасности и защиты
2	Административный уровень обеспечения информационной безопасности
3	Контроль за соблюдением требований информационной безопасности и защиты информации
4	Анализ угроз. Проблемы безопасности IP-сетей. Пути решения проблем защиты информации в сетях. Политика безопасности
5	Простая аутентификация. Строгая аутентификация. Биометрическая аутентификация

Типовой тест промежуточной аттестации

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

a) Разработка аппаратных средств обеспечения правовых данных
b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

a) Хищение жестких дисков, подключение к сети, инсайдерство
b) Перехват данных, хищение данных, изменение архитектуры системы
c) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

a) Персональная, корпоративная, государственная
b) Клиентская, серверная, сетевая
c) Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

a) несанкционированного доступа, воздействия в сети
b) инсайдерства в организации
c) чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

a) Компьютерные сети, базы данных
b) Информационные системы, психологическое состояние пользователей
c) Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

a) Искажение, уменьшение объема, перекодировка информации
b) Техническое вмешательство, выведение из строя оборудования сети
c) Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

a) Экономической эффективности системы безопасности
b) Многоплатформенной реализации системы
c) Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

a) руководители, менеджеры, администраторы компаний
b) органы права, государства, бизнеса
c) сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

a) Установление регламента, аудит системы, выявление рисков
b) Установка новых офисных приложений, смена хостинг-компании
c) Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

a) Неоправданных ограничений при работе в сети (системе)
b) Рисков безопасности сети, системы
c) Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

a) Невозможности миновать защитные средства сети (системы)
b) Усиления основного звена сети, системы
c) Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

a) Усиления защищенности самого незащищенного звена сети (системы)
b) Перехода в безопасное состояние работы сети, системы
c) Полного доступа пользователей ко всем ресурсам сети, системы

3) Принципом политики информационной безопасности является принцип:

a) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
b) Одноуровневой защиты сети, системы
c) Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

a) Компьютерный сбой
b) Логические закладки («мины»)
c) Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

a) Прочитать приложение, если оно не содержит ничего ценного – удалить
b) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
c) Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

a) Секретность ключа определена секретностью открытого сообщения
b) Секретность информации определена скоростью передачи данных
c) Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

a) Электронно-цифровой преобразователь
b) Электронно-цифровая подпись
c) Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

a) Покупка нелицензионного ПО
b) Ошибки эксплуатации и неумышленного изменения режима работы системы
c) Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

a) Распределенный доступ клиент, отказ оборудования
b) Моральный износ сети, инсайдерство
c) Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

a) Слабый трафик, информационный обман, вирусы в интернет
b) Вирусы в сети, логические мины (закладки), информационный перехват
c) Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

a) Потерей данных в системе
b) Изменением формы информации
c) Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

a) Целостность
b) Доступность
c) Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

a) Вероятное событие
b) Детерминированное (всегда определенное) событие

c) Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

a) Регламентированной
b) Правовой
c) Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

a) Программные, технические, организационные, технологические
b) Серверные, клиентские, спутниковые, наземные
c) Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

a) Владелец сети
b) Администратор сети
c) Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

a) Руководств, требований обеспечения необходимого уровня безопасности
b) Инструкций, алгоритмов поведения пользователя в сети
c) Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

a) Аудит, анализ затрат на проведение защитных мер
b) Аудит, анализ безопасности
c) Аудит, анализ уязвимостей, риск-ситуаций

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.Итоговый контрольный тест доступен студенту только во время тестирования, согласно расписанию занятий или в установленное деканатом время.
2.Студент информируется о результатах текущей успеваемости.
3.Студент получает информацию о текущей успеваемости и допуске к процеду-

ре итогового тестирования от преподавателя или в ЭИОС.
4.Производится идентификация личности студента.
5.Студентам, допущенным к промежуточной аттестации, открывается итоговый контрольный тест.
6.Тест закрывается студентом лично по завершении тестирования или автоматически по истечении времени тестирования.

Опрос устный

Опрос устный - диалог преподавателя со студентом, цель которого - систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала.

Устный опрос по основным терминам может проводится в начале/конце лекционного или практического занятия в течение 15 -20 мин. Либо устный опрос проводится в течение всего практического занятия по заранее выданной тематике. Выбранный преподавателем студент может отвечать с места либо у доски.

Критериями оценки устного опроса являются: правильность ответа на вопросы, степень раскрытия сущности вопроса.

Оценка **«отлично»** — дан полный, всесторонний ответ на вопрос. Точность в определениях. Приведение примеров из практики.

Оценка **«хорошо»** — дан неполный ответ на вопрос. Допущены неточности при ответе. Допущены неточности в основных определениях.

Оценка **«удовлетворительно»** — имеются существенные недочеты при ответе. Вопрос раскрыт частично. Незнание базовых определений курса.

Оценка **«неудовлетворительно»** — вопрос не раскрыт или дан неверный ответ.

Тесты

Тесты - инструмент, с помощью которого педагог оценивает степень достижения студентом требуемых знаний, умений, навыков. Составление теста включает в себя создание выверенной системы вопросов, собственно процедуру проведения тестирования и способ измерения полученных результатов.

Критерии оценки теста: Оценка **«отлично»** выставляется при условии правильного ответа студента не менее чем 85 % тестовых заданий;

Оценка **«хорошо»** выставляется при условии правильного ответа студента не менее чем 70 % тестовых заданий;

Оценка **«удовлетворительно»** выставляется при условии правильного ответа студента не менее 51 %; .

Оценка **«неудовлетворительно»** выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.

Контрольная работа

Контрольная работа - средство промежуточного контроля остаточных знаний и умений, состоит из вопросов или заданий, которые студент должен решить, выполнить. Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме.

Критерии оценки контрольной работы для студентов заочного отделения:
Оценка «зачтено» ставится за полные ответы на все вопросы.
Оценка «не зачтено» ставится, если освещены не все вопросы требуемого материала или не описано главное в содержании вопросов, или письменная работа не сдана.

Коллоквиум (в переводе с латинского «беседа, разговор») – форма текущего контроля знаний студентов, которая проводится в виде собеседовании преподавателя и студента по самостоятельно подготовленной студентом теме.

Он применяется для проверки знаний по определенному разделу (или объемной теме) и принятия решения о том, можно ли переходить к изучению нового материала. Коллоквиум — это беседа со студентами, целью которой является выявление уровня овладения новыми знаниями. В отличие от семинара главное на коллоквиуме — это проверка знаний с целью их систематизации.

Целью коллоквиума является формирование у студента навыков анализа теоретических проблем на основе самостоятельного изучения учебной и научной литературы.

На коллоквиум выносятся крупные, проблемные, нередко спорные теоретические вопросы. Коллоквиум может проводиться по вопросам, обсуждавшимся на семинарах. Конкретные вопросы для коллоквиума студентам не сообщаются, однако заранее формулируются преподавателем. Предполагаемый объем ответа не должен быть большим (примерно 1,5-2 минуты), чтобы преподаватель мог успеть опросить всех студентов.

От студента требуется:

- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.

Коллоквиум — это не только форма контроля, но и метод углубления, закрепления знаний студентов, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у студента в процессе изучения данного источника.

Задача коллоквиума добиться глубокого изучения отобранного материала, пробудить у студента стремление к чтению дополнительной экономической литературы.

Подготовка к проведению коллоквиума.

Подготовка к коллоквиуму предполагает несколько этапов:

1. Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума.

2. Как правило, на самостоятельную подготовку к коллоквиуму студенту отводится 3–4 недели. Подготовка включает в себя изучение рекомендованной литературы и (по указанию преподавателя) конспектирование важнейших источников.

3. Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах (3–5 человек).

4. Преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, контролирует конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания.

5. По итогам коллоквиума выставляется дифференцированная оценка, имеющая большой удельный вес в определении текущей успеваемости студента.

Особенности и порядок сдачи коллоквиума. Студент может себя считать готовым к сдаче коллоквиума по избранной работе, когда у него есть им лично составленный и обработанный конспект сдаваемой работы, он знает структуру работы в целом, содержание работы в целом или отдельных ее разделов (глав); умеет раскрыть рассматриваемые проблемы и высказать свое отношение к прочитанному и свои сомнения, а также знает, как убедить преподавателя в правоте своих суждений.

Проведение коллоквиума позволяет студенту приобрести опыт работы над первоисточниками, что в дальнейшем поможет с меньшими затратами времени работать над литературой по курсовой работе и при подготовке к экзаменам.

Экзамен

Экзамен - итоговая форма оценки знаний.

Проводится в заданный срок, согласно графику учебного процесса.

Критерии оценки при проведении экзамена:

Оценка "отлично" ставится, если студент обнаружил полное знание учебно-программного материала, успешно выполняет предусмотренные в программе задания, усвоил основную литературу, рекомендованную в программе. Ответ полный и правильный на основании изученного материала. Выдвинутые

положения аргументированы и иллюстрированы примерами. Материал изложен в определенной логической последовательности, осознанно, литературным языком, с использованием современных научных терминов; ответ самостоятельный. Студент уверенно отвечает на дополнительные вопросы

Оценка «хорошо» ставится в том случае, когда студент обнаруживает полное знание учебного материала, демонстрирует систематический характер знаний по дисциплине. Ответ полный и правильный, подтвержден примерами; но их обоснование не аргументировано, отсутствует собственная точка зрения. Материал изложен в определенной логической последовательности, при этом допущены 2-3 несущественные погрешности, исправленные по требованию экзаменатора. Студент испытывает незначительные трудности в ответах на дополнительные вопросы. Материал изложен осознанно, самостоятельно, с использованием современных научных терминов, литературным языком.при этом могут допускаться некоторые погрешности в ответе на зачете, если студент обладает необходимыми знаниями для их устранения под руководством преподавателя.

Оценка «удовлетворительно» ставится в том случае, когда студент обнаруживает знание основного программного материала по дисциплине, но допускает погрешности в ответе. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены правильно, но обнаруживается недостаточное раскрытие теоретического материала. Выдвигаемые положения недостаточно аргументированы и не подтверждены примерами; ответ носит преимущественно описательный характер. Студент испытывает достаточные трудности в ответах на вопросы. Научная терминология используется недостаточно.

Оценка «неудовлетворительно» выставляется студенту, обнаружившему проблемы в знаниях основного учебного материала по дисциплине. При ответе обнаружено непонимание студентом основного содержания теоретического материала по дисциплине. При ответе обнаружено непонимание студентом основного содержания теоретического материала или допущен ряд существенных ошибок, которые студент не может исправить при наводящих вопросах экзаменатора. Студент подменил научное обоснование проблем рассуждением бытового плана. Ответ носит поверхностный характер; наблюдаются неточности в использовании научной терминологии.

7. Учебно-методическое и материально-техническое обеспечение дисциплины «Методы и средства защиты информации»

7.1. Учебная литература:

Основная литература:

1. Бабаш А. В., Ларин Д. А. История защиты информ.в за-руб.странах:Уч.пос./А.В.Бабаш-ИЦ РИОР,НИЦ ИНФРА-М,2016-283с (ВОБакалавр.(о); Высшая школа - Москва, 2021. - 627 с.
2. Петраков А. В. Основы практической защиты информации; РадиоСофт - М., 2020. - 504 с.
3. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. Учебное пособие; Ленанд - М., 2018. - 248 с.
4. Лапонина О. Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия; Интернет-университет информационных технологий, Бином. Лаборатория знаний - М., 2019. - 536 с.

Дополнительная литература:

1. Мельников Д. А. Информационная безопасность открытых систем: моногр. ; Флинта, Наука - М., 2019. - 448 с.
2. Партыка Т. Л., Попов И. И. Информационная безопасность; Форум - М., 2022. - 432 с.
3. Проскурин В. Г. Защита в операционных системах. Учебное пособие; Гостехиздат - Москва, 2022. - 192 с.
4. Хорев П. Б. Программно-аппаратная защита информации; Форум - М., 2020. - 352 с.

7.2. Интернет-ресурсы

1. Электронная информационно-образовательная среда АНО ВО "СЗТУ" (ЭИОС СЗТУ) [Электронный ресурс]. - Режим доступа: http: //edu.nwotu.ru/
2. Учебно-информационный центр АНО ВО "СЗТУ" [Электронный ресурс]. - Режим доступа: http://lib.nwotu.ru:8087/iirbis2/
3. Электронно-библиотечная система IPRbooks[Электронный ресурс]. - Режим доступа:http: //www.iprbookshop. ru/
4. Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный ресурс]. - Режим доступа: http: //window.edu.ru/
5. Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН) [Электронный ресурс]. - Режим доступа: http: //www.vlibrary.ru/

7.3. Программное обеспечение

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

Internet - технологии:

WWW (англ. WorldWideWeb- Всемирная Паутина) - технология работы в сети с гипертекстами;

FTP (англ. FileTransferProtocol- протокол передачи файлов) - технология передачи по сети файлов произвольного формата;

IRC (англ. InternetRelayChat- поочередный разговор в сети, чат) - технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога;

ICQ (англ. Iseekyou - я ищу тебя, можно записать тремя указанными буквами) - технология ведения переговоров один на один в синхронном режиме.

1. Дистанционное обучение с использованием ЭИОС на платформе Moodle.
2. Технология мультимедиа в режиме диалога.
3. Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории).
4. Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.

Программное обеспечение: ППП MSOffice2010

7.4. Материально-техническое обеспечение

Описание материально-технической базы, необходимой для изучения модуля

Перечень материально-технического обеспечения

№ п/п	Вид занятий	Вид и наименование оборудования
1	Лекционные занятия	Аудитории с мультимедийными средствами, средствами звуковоспроизведения и имеющие выход в сеть «Интернет». Помещения для проведения аудиторных занятий, оборудованные учебной мебелью
2	Лабораторные работы	Компьютерный класс с комплексом программных средств, позволяющих каждому студенту разрабатывать программные реализации практических задач в ходе выполнения лабораторных работ
3	Самостоятельная работа	Библиотека, имеющая рабочие места для студентов. Аудитории, оснащенные компьютерами с доступом к сети «Интернет»
4	Практика	Компьютерный класс с комплексом программных средств, позволяющих каждому студенту разрабатывать программные реализации практических задач в ходе выполнения лабораторных работ

Рабочая программа дисциплины «Методы и средства защиты информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 926.

Программу составил: старший преподаватель кафедры «Информационные системы и технологии», _____/ Цуроев И.М.

Программа одобрена на заседании кафедры «Информационные системы и технологии»

Протокол № 10 от «21» июня 2023 года

Программа одобрена Учебно-методическим советом физико-математического факультета

Протокол № 10 от «23» июня 2023 года

Программа рассмотрена на заседании Учебно-методического совета университета

Протокол № 10 от «28» июня 2023 года

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой