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

АННОТАЦИЯ

рабочей программы учебной дисциплины
Б1.В.ДВ.05.01 Методы и средства защиты информации

Направление подготовки (*бакалавриат)*
09.03.02 «Информационные системы и технологии»

1.	**Цель изучения дисциплины** Целями освоения дисциплины«Методы и средства защиты информации» являются фо безопасности и применения на практике методов и средств защиты информации
2.	**Место дисциплины в структуре ОПОП ВО (*бакалавриата)*** Дисциплина «Методы и средства защиты информации» изучается в блоке Б1.В и являетс образовательных отношений и имеет соответствующий шифр Б1.В.ДВ.05.01 подготовки бакалаврия Дисциплины и практики, знания и умения по которым необходимы как "входные" при изучении дан Дисциплины, практики, ГИА, для которых изучение данной дисциплины необходимо как «предшес Управление данными, Защита интеллектуальной собственности, Корпоративные информационныес Качественное освоение дисциплины «Методы и средства защиты информации» также необходи работы.
3.	**Результаты освоения дисциплины (модуля) «**Методы и средства защиты информации**»**

Код и наименование компетенции	Индикаторы
	Общепрофессиональные компетен
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1.: понимает виды ресурсов и огран решения профессиональных задач; основн оценки разных способов решения задач; д законодательство и правовые нормы, ре профессиональную деятельность. УК-2.2.:проводит анализ поставленной формулировать задачи, которые необходимо р ее достижения; анализировать альтернативны для достижения намеченных результатов; ис нормативно-правовую документацию н профессиональной деятельности.
	Общепрофессиональные компетен

	ОПК-4 Способен участвовать вразработкетехническойдокументациисвязанной с профессиональнойдеятельностью с использованием стандартов нормиправил	ОПК-4.1.: Понимает основные стандарты оформлениятехническойдокументациинаразлич жизненного циклаинформационной системы. ОПК-4.2.Применяет стандартыоформления техн документации на различныхстадиях жизненного циклаинформационной системы. ОПК-4.3.Осуществляет составление техническойдокументации на этапахжизненного цикла информационнойсист
	Профессиональные компетенци	
	ПК-4 Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПК-4.1:Используетспециальные знания по рабо установленной БД; общие основы решения прак задач по восстановлению БД и проверке коррек восстановленных данных; основы управления у записями пользователей; ПК-4.2: выполняет регламентные процедуры по резервированию данных; выбирать способ дейст известных; контролировать, оценивать и коррек свои действия; выполнять регламентные проце восстановлению и проверке корректности восст данных; выбирать способ действия из известны контролировать, оценивать и корректировать св действия; применять специальные процедуры у правами доступа пользователей. ПК-4.3: запускает процедуры резервного копир мониторинга выполнения процедуры резервного копирования; контроля завершения процедуры копирования; запуска процедуры восстановлени мониторинга выполнения процедуры восстанов контроля завершения процедуры восстановлени назначения прав доступа пользователей к БД; из прав доступа пользователей к БД; контроля соб прав доступа пользователей к БД
	ПК-8Способность выполнять работы по разработке компонентов системных программных продуктов: компиляторов, загрузчиков, сборщиков, системных утилит, драйверов устройств, по созданию инструментальных средств программирования	ПК-8.1.:понимает синтаксис выбранного языка программирования, особенности программиров этом языке, стандартные библиотеки языка программирования; методологии разработки пр обеспечения; методологии и технологии проект использования баз данных; технологии програм особенности выбранной среды программирован системы управления базами данных; компонент программно-технических архитектур, существу

		приложения и интерфейсы взаимодействия с ни ПК-8.2: применяет выбранные языки программ для написания программного кода; использоват выбранную среду программирования и средства управления базами данных; использовать возмо имеющейся технической и/или программной ар

4. Структура и содержание дисциплины

4.1. Структура дисциплины

Вид учебной работы	Всего	Порядковый номер семестра			
		5			
Общая трудоемкость дисциплины всего (в з.е.), в том числе:	3				
Курсовой проект (работа)					
Аудиторные занятия всего (в акад. часах), в том числе:	50	50			
Лекции	18	18			
Практические занятия, семинары					
Лабораторные работы	32	32			
Самостоятельная работа всего (в акад. часах), в том числе:	58	58			
КСР					
Зачет	5				
Общая трудоемкость дисциплины	108	108			

4.2. Содержание дисциплины

Тема 1. Понятие и сущность информационной безопасности и защиты информации.

Необходимость и значимость нормативно-правового определения основных понятий. Понятие
компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие по
общества. Базовые уровни обеспечения ИБ и защиты информации.

Тема 2. Основные угрозы информационной безопасности.

Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способ
зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкц
Базовые принципы защиты от несанкционированного доступа к информации в соответствии с
реализации угроз.

Тема 3. Правовой уровень обеспечения информационной безопасности.

Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые а
комиссии по защите государственной тайны в формировании перечня сведений, составляю
предпринимательской деятельности. Основания и методика отнесения сведений к коммерч
коммерческую тайну. Методика формирования на фирме перечня сведений, относящихся к коммерч

Тема 4. Административный уровень обеспечения информационной безопасности.

Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как
Структура документа, характеризующего политику безопасности, и основные этапы разработки
методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и ан
управления рисками. Основные принципы реализации ПИБ.

	Тема 5.Программно-технический уровень обеспечения защиты информации. Программные сервисы защиты информации в ИС. Идентификация и аутентификация пользователе аутентификации. Модели разграничения доступа к информации. Протоколирование и аудит (актив криптографического преобразования данных. Потоковое и блочное шифрование. Процедура информационнотелекоммуникационных сетях (ИТС). Основные сервисы защиты в ИТС. Компь средства борьбы с ними. Антивирусные программные комплексы. **Тема 6. Процедурный уровень информационной безопасности.** Основные классы мер процедурного уровня Управление персоналом Физическая защита Поддержа Планирование восстановительных работ. **Тема 7.Система защиты информации.** Процесс развития средств и методов защиты информации Этапы развития системы защиты инфо защиты информации Системный подход к построению системы защиты информации Цели задач созданию системы защиты информации. Структура систем защиты информации на современном эта **Тема 8.Обеспечение режима конфиденциально сти при работе с защищаемой информацией** Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиден лиц, работников к конфиденциальной информации Доступ должностных лиц, работников к ко должностных лиц, допущенных к сведениям, составляющим коммерческую тайну Порядок пр сторонних организаций, государственным учреждениям. **Тема 9. Контроль за соблюдением требований информационной безопасности и защиты инфор** Основные положения по осуществлению контроля, назначение, цель и задачи контроля. Основные (контроля) наличия документов и иных носителей информации ограниченного доступа Провед информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений **Тема 10. Ответственность за правонарушения информационной безопасности и защиты инфо** Понятие и виды юридической ответственности за нарушение правовых норм по защите информаци Административная ответственность за правонарушения в области защиты интеллектуальной собст правонарушения в области защиты государственной тайны Уголовная ответственность за правонару
5.	**Образовательные технологии** В освоении дисциплины используются следующие образовательные технологии: • Компьютерные классы с набором лицензионного базового программного обеспечениядляпроведе • Skype,ЭИОС на платформе Moodle дляпроведениядистанционногообучениияиконсультаций. • Технология мультимедиа в режиме диалога. • Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатор • 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;
6.	**Используемые ресурсы информационно-телекоммуникационной сети «Internet»; информационные тех**

	1.Электронная информационно-образовательная среда АНО ВО "СЗТУ" (ЭИОС СЗТУ) [Электронн 2.Учебно-информационный центр АНО ВО "СЗТУ" [Электронный ресурс]. - Режим доступа: http://l 3.Электронно-библиотечная система IPRbooks [Электронный ресурс]. - Режим доступа: http://www.i 4.Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный рес 5.Информационная системы доступа к электронным каталогам библиотек сферы образован http://www.vlibrary.ru/
7.	**Формы текущего контроля**
	Коллоквиумы, тесты, лабораторные работы по разделам дисциплины
8.	**Форма промежуточного контроля**
	Зачет

Разработчик: ст.преподаватель кафедры математики и ИВТУжахова М.М.