Министерство науки и высшего образования Российской Федерации
Федеральное Государственное Бюджетное Образовательное
Учреждение Высшего Образования
«Ингушский Государственный Университет»

Принята
решением Ученого совета ИнгГУ

от «30» июня 2022г.
Протокол №10

Утверждаю
И.о. проректора по УР_____Ф.Д. Кодзоева

«30» июня 2022г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

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

Направленность (*профиль подготовки*)
Информационные системы и технологии

Квалификация выпускника
бакалавр

Форма обучения
очная

Магас, 2022

1. Цели освоения дисциплины

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 дисциплины в структуре ОПОП 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 – зачет.

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:

Код компетенции	Наименование компетенции	Индикатор достижения компетенции	В результате освоения дисциплины обучающийся **должен**:
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 ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную 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.	Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. Уметь: проводить 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.
ОПК-4	Способен участвовать в разработке технической документации связанной с профессиональной деятельностью с использованием стандартов норм и правил	ОПК-4.1.: Понимает основные стандарты оформления технической документации на различныхстадиях жизненного цикла информационной системы. ОПК-4.2. Применяет стандарты оформления технической документации на различныхстадиях жизненного цикла информационной системы.	Знать основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. Уметь применять стандарты оформления технической документации на различных стадиях жизненного цикла информа-ционной системы.

		ОПК-4.3.Осуществляет составление технической документации на различных этапах жизненного цикла информационной системы	Владеть навыками составления технической документации на различных этапах жизненного цикла информационной системы
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; контроля завершения процедуры восстановления БД; назначения прав доступа пользователей к БД; изменения прав доступа пользователей к БД; контроля соблюдения прав доступа пользователей к БД.	Знать: специальные знания по работе с установленной БД; общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных; специальные знания по работе с установленной БД; основы управления учетными записями пользователей; специальные знания по работе с установленной БД. Уметь: выполнять 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; Владеть навыками: запуска процедуры резервного копирования; мониторинга выполнения процедуры резервного копирования; контроля завершения процедуры резервного копирования; запуска процедуры восстановления БД; мониторинга выполнения процедуры восстановления БД; контроля завершения процедуры восстановления БД; назначения прав доступа пользователей к БД; изменения прав доступа пользователей к

			БД; контроля соблюдения прав доступа пользователей к БД.
ПК-8	Способность 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 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 Б1.В.ДВ.05.01 Методы и средства защиты информации

Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

№ п/п	Наименование разделов и тем дисциплины (модуля)	семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в		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.	Всего	Курсовая работа(проект)	Подготовка к экзамену	Другие виды самостоятельнойра	Собеседование	Коллоквиум	Проверка тестов	Проверка контрольн. работ	Проверка доклада	Проверка эссе и иных творческих	курсовая работа (проект)
1.	Тема 1. Понятие и сущность информационной безопасности и защиты	5	4	2				2			2							
2.	Тема 2. Основные угрозы информационной безопасности	5	4	2				2			2							
3.	Тема 3.Правовой уровень обеспечения информационной безопасности	5	4	2				2			2							
4.	Тема 4. Административный уровень обеспечения информационной безопасности	5	20	2		8		10			10							
5.	Тема 5. Программно-технический уровень обеспечения защиты информации	5	20	2		8		10			10							
6.	Тема 6. Процедурный уровень информационной безопасности	5	12	2				10			10							
7.	Тема 7. Система защиты информации	5	10	2		8		4			4							
8.	Тема 8. Обеспечение режима конфиденциальности при работе с защищаемой информацией	5	22	2		4		10			10							
9.	Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации	5	9	1		4		4			4							
10.	Тема 10. Ответственность за правонарушения информационной безопасности и защиты информации	5	5	1				4			4							

	Общая трудоемкость, в часах		108	18		32		50			58	Промежуточная	
												Форма	
												Зачет	x
												Зачет с оценкой	
												Экзамен	

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 воз-действия 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 в 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 конфиденциально сти 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.

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;
- зачет.

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 р уководстве 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

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	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

	информационной безопасности				
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	10
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	10
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

Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов организуется в компьютерном классе с развернутой ЛВС, имеющей подключение к сети Интернет и обеспечивающей доступ к ресурсам электронного обучения, современным профессиональным базам данных и информационным справочным системам.

Рекомендуется проведение следующих видов самостоятельной работы:

- подготовка к практическим занятиям: изучить теоретический материал по теме практического занятия, ответить на контрольные вопросы;

- подготовка статьи на студенческую конференцию ФВТ: изучить литературу по выбранной теме, обобщить материал, изучить требования к оформлению статьи, представить оформленную статью;

- работа с конспектом лекций и изучение рекомендованной литературы: изучить конспект лекций, ответить на контрольные вопросы, изучить разделы рекомендованной литературы;

- подготовка к зачету: повторить материал, изученный в течение семестра, студентам из числа лиц с ограниченными возможностями здоровья могут быть предложены электронные образовательные ресурсы в формах, адаптированных к ограничениям их здоровья.

Материалы для проведения текущего и промежуточного контроля знаний студентов

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1.	Лабораторная работа. Коллоквиум.	Тема 1. Понятие и сущность информационной безопасности и защиты информации Тема 2. Основные угрозы информационной безопасности Тема 3.Правовой уровень обеспечения информационной безопасности Тема 4. Административный уровень обеспечения информационной безопасности	УК-2, ПК-4, ПК-8, ОПК-4
2.	Лабораторная работа. Контрольный тест	Тема 5. Программно-технический уровень обеспечения защиты информации Тема 10.Ответственность за правонарушения информационной безопасности и защиты информации	УК-2, ПК-4, ПК-8, ОПК-4
3.	Лабораторная работа. Коллоквиум.	Тема 6.Процедурный уровень информационной безопасности Тема 7.Система защиты информации Тема 8. Обеспечение режима конфиденциально сти при работе с защищаемой информацией Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации	УК-2, ПК-4, ПК-8, ОПК-4

7. Учебно-методическое и материально-техническое обеспечение дисциплины

При изучении дисциплины для проработки всех тем и выполнения заданий по всем темам студенты могут использовать различные учебно-методические материалы, размещаемые в электронном виде преподавателями, которая предполагает также возможность обмена информацией с преподавателем для подготовки заданий.

Материально-техническое обеспечение образовательного процесса по дисциплине Методы и средства защиты информации включает в себя следующие компоненты:

- Учебные аудитории для контактной работы с преподавателем, укомплектованных специализированной мебелью (столы и стулья).Компьютерные классы с набором лицензионного базового программного обеспечения для проведения лабораторных занятий с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду;
- Дополнительные мультимедийные материалы, мультимедийная аудитория;

Skype, для проведения дистанционного обучения и консультаций

Учебная литература:

№	Автор	Название	Издательство	Год издания	Вид издания	Кол-во в библиотеке	Адрес электронного ресурса	Вид доступа
1	2	3	4	5	6	7	8	9
Основная литература								
7.1.1.	Башлы П.Н. Бабаш А.В. Баранова Е.К.	Информационная безопасность и защита информации	Евразийский открытый институт	2012	учебное пособие	-	http://www.iprbookshop.ru/10677.html	по логину и паролю
7.1.2.	Спицын В.Г.	Информационная безопасность вычислительной техники	Томский государственный университет систем управления и радиоэлектроники, Эль Контент	2011	учебное пособие	-	http://www.iprbookshop.ru/13936.html	по логину и паролю
7.1.3.	Е.Б.Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М.	Основы информационной безопасности	Горячая линия - Телеком,	2011.	Учебное пособие для вузов	-	http://www.studentlibrary.ru/book/ISBN5935172925.html (ЭБС «Консультант студента»).	-
Дополнительная литература								
7.1.4.	Андрианов В.В. Зефиров С.Л.	Обеспечение информационно й	ЦИПСиР	2011	энцикло педия -	-	http://www.iprbookshop.ru/38525.html	по логину и

	Голованов В.Б. Голдуев Н.А.	безопасности бизнеса						парол ю
7.1.5.	Голиков А.М.	Основы информацион но й безопасности	Томский государст венный университ ет систем управлени я и радиоэлек троники	2007	учебное пособие	-	http://www. iprbookshop.ru /13957.html	по логину и парол ю
7.1.6.	Дождиков В.Г. Салтан М.И.	Краткий энциклопеди чес кий словарь по информацион но й безопасности	Энергия	2010	энцикло педичес кий словарь	-	http://www. iprbookshop.ru /5729.html	по логину и парол ю

Интернет-ресурсы

Название ресурса	Ссылка/доступ
Электронная библиотека онлайн «Единое окно Образовательным ресурсам»	http://window.edu.ru
«Образовательный ресурс России»	http://school-collection.edu.ru
Федеральный образовательный портал: учреждения, программы, стандарты, ВУЗы, тесты ЕГЭ, ГИА	http://www.edu.ru–
Федеральный центр информационно-образовательных ресурсов (ФЦИОР)	http://fcior.edu.ru-
ЭБС "КОНСУЛЬТАНТ СТУДЕНТА". Электронная библиотека технического вуза	http://polpred.com/news
Издательство «Лань». Электронно-библиотечная система	http://www.studentlibrary.ru-
Русская виртуальная библиотека	http://rvb.ru–
Кабинет русского языка и литературы	http://ruslit.ioso.ru–
Национальный корпус русского языка	http://ruscorpora.ru–
Издательство «Лань». Электронно-библиотечная система	http://e.lanbook.com-
Еженедельник науки и образования Юга России «Академия»	http://old.rsue.ru/Academy/Archives/Index.htm
Научная электронная библиотека«e-Library»	http://elibrary.ru/defaultx.asp-
Электронно-библиотечная система IPR books	http://www.iprbookshop.ru-
Электронно-справочная система документов в сфере образования «Информио»	http://www.informio.ru
Информационно-правовая система «Консультант-плюс»	Сетевая версия, доступна со всех компьютеров в корпоративной сети ИнгГУ
Информационно-правовая система «Гарант»	Сетевая версия, доступна со всех компьютеров в корпоративной сети ИнгГУ
Электронно-библиотечная система «Юрайт»	https://www.biblio-online.ru

Программное обеспечение

Лицензионное программно-информационное обеспечение	1. Microsoft Windows 2. Microsoft Office

	3. Google Chrome 4. Консультант+ 5. Антиплагиат.ВУЗ

Материально-техническое обеспечение

Для проведения лекций по дисциплине используются специализированные аудитории с мультимедийным оборудованием или с возможностями подключения к такому оборудованию, позволяющему демонстрировать на большом экране приемы работы с персональным компьютером и другой лекционный материал (технические характеристики компьютера, входящего в состав мультимедийного оборудования или используемого совместно с таким оборудованием, должны обеспечивать возможность работы с современными версиями ОС Windows, пакета Microsoft Office, обслуживающих, прикладных программ и другого ПО).

Для проведения лабораторных занятий по дисциплине и для самостоятельной работы студентов используются специализированные аудитории, оснащенные персональными компьютерами, при проведении лабораторных занятий используются современное программное обеспечение (операционную систему Windows 7 и выше, пакет Microsoft Office 2010 и выше, а также обслуживающие программы и среды разработки программ по выбору преподавателей).

Рабочая программа дисциплины Б1.В.ДВ.05.01 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, с учетом примерной программы учебной дисциплины из ПООП.

Программу составила :
Ст.преподаватель, М.и. Мурзабекова

Программа одобрена на заседании кафедры « Информационные системы и технологии»
Протокол № 10 от «20» июня 2022г.

Программа одобрена Учебно-методическим советом физико-математического факультета
Протокол № 1 от «22» июня 2022г.

Программа одобрена на заседании Учебно-методического совета университета
Протокол № 10 от «29» июня 2022г.

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

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