МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Физико-технический факультет

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУ ЛЯ)

ФТД.02 Информационная безопасность

Направление подготовки/специальность 03.03.02 Физика, 03.03.03 Радиофизика, 12.03.02 Биотехнические системы и технологии, 11.03.01 Радиотехника, 11.03.02 Инфокоммуникационные технологии и системы связи, 11.03.04 Электроника и наноэлектроника09.03.02 Информационные системы и технологии,

Форма обучения очная

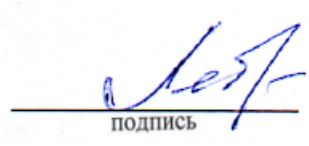
Квалификация бакалавр

Краснодар 2025

Рабочая программа дисциплины ФТД.02 Информационная безопасность, составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки/ специальности 03.03.02 Физика, 03.03.03 Радиофизика, 12.03.02 Биотехнические системы и технологии, 11.03.01 Радиотехника, 11.03.02 Инфокоммуникационные технологии и системы связи, 11.03.04 Электроника и наноэлектроника, 09.03.02 Информационные системы и технологии

Программу составил (и):
Н.Н. Куликова, доцент кафедры теор. физики и комп. тех
кандидат биолог. наук

Рабочая программа дисциплины ФТД.02 Информационная безопасность
утверждена на заседании кафедры теоретической физики и компьютерных технологий
протокол № 9 от «08» апреля 2025 г.
Заведующий кафедрой (выпускающей) Лебедев К.А.



Утверждена на заседании учебно-методической комиссии физико-технического факультета
протокол № 11 от « 21 » апреля 2025 г.
Председатель УМК факультета Богатов Н.М.

Рецензенты:

М.С. Коваленко, кандидат физико-математических наук, доцент кафедры физики и информационных систем

Л.Р. Григорян, генеральный директор ООО НПФ «Мезон»
кандидат физико-математических наук

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Формирование у студентов компетенций в области основных принципов, методов, способов и средств защиты информации, а также их применения в корпоративных информационно-технологических системах.

1.2 Задачи дисциплины.

1) изучение и классификация причин нарушений безопасности, методов и средств защиты информации;

2) рассмотрение области применения и тенденций развития средств защиты информации;

3) приобретение практических навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации, проектирование мониторов безопасности субъектов и объектов.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к факультативным дисциплинам.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Код и наименование индикатора*	Результаты обучения по дисциплине
ПК-3 Способность проводить эффективный поиск, критически анализировать, интерпретировать и управлять информацией в цифровой среде с соблюдением принципов цифровой безопасности и кибергигиены.	
ПК-3.3 знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски, а также способы нейтрализации этих рисков, включая защиту от кибератак, вредоносного программного обеспечения, фишинга и других угроз, связанных с цифровым миром	Знать различных видов угроз, методы и инструменты защиты информации, стандарты и нормативные акты, подходы к управлению рисками, включая оценку уязвимостей, анализ угроз и разработку стратегий по минимизации рисков
	Уметь проводить анализ систем на наличие уязвимостей, использование инструментов для сканирования и тестирования на проникновение, отслеживать и анализировать новые угрозы в сфере кибербезопасности, проводить обучение и просвещение пользователей о безопасном поведении в сети, включа я распознавание фишинга и безопасное использование паролей
	Владеть навыками работы с современными инструментами и технологиями, такими как облачные решения, блокчейн, искусственный интеллект и машинное обучение для повышения уровня безопасности

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часа), их распределение по видам работ представлено в таблице

Вид учебной работы	Всего часов	Семестры (часы)			
		8			
Контактная работа, в том числе:	**24,2**	**24,2**			
Аудиторные занятия (всего):	**24**	**24**			

Занятия лекционного типа		12	12			
Лабораторные занятия						
Занятия семинарского типа (семинары, практические занятия)		12	12			
Иная контактная работа:		**2,2**	**2,2**			
Контроль самостоятельной работы (КСР)		2	2			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**45,8**	**45,8**			
Проработка учебного (теоретического) материала		45,8	45,8			
Общая трудоемкость	**час.**	**72**	**72**			
	в том числе контактная работа	**24,2**	**24,2**			
	зач. ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 8 семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Тема 1. Актуальность информационной безопасности, понятия и определения	8	2	2		8
2.	Тема 2. Угрозы информации	8	2	2		8
3.	Тема 3. Организационно-правовая защита информации	16	4	4		8
4.	Тема 4. Программная защита информации	16	4	4		8
5.	Тема 5. Техническая защита информации	8	2	2		8
6.	Тема 6. Цифровая гигиена	8	2	2		5,8
	ИТОГО по разделам дисциплины	69,8	12	12		45,8
	Контроль самостоятельной работы (КСР)	2				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Тема 1. Актуальность информационной	1.1. Актуальность информационной безопасности.	опрос

	безопасности, понятия и определения	1.2. Национальные интересы РФ в информационной сфере и их обеспечение. 1.3. Классификация компьютерных преступлений. 1.4. Способы совершения компьютерных преступлений. 1.5. Пользователи и злоумышленники в Интернет. 1.6. Причины уязвимости сети Интернет.	
2.	Тема 2. Угрозы информации	2.1. Виды угроз информационной безопасности РФ. 2.2. Источники угроз информационной безопасности РФ. 2.3. Угрозы информационной безопасности для АСОИ. 2.4. Удаленные атаки на интрасети.	опрос
3.	Тема 3. Организационно-правовая защита информации	3.1. Организационные меры по защите информации. Политики и процедуры безопасности информации. 3.2. Организационные мероприятия по защите информации. Организация информационной безопасности компании. Оценка рисков и управление инцидентами. 3.3. Методы повышения осведомленности сотрудников о рисках, связанных с обработкой информации. 3.4. Международное сотрудничество в области защиты информации	опрос
4.	Тема 4. Программная защита информации	4.1. Введение в программную защиту информации. Управление доступом и аутентификация. Электронная цифровая подпись. 4.2. Шифрование и криптография 4.3. Безопасность веб-приложений. Безопасность мобильных приложений 4.4. Источники компьютерных вирусов. Признаки заражения компьютера. Антивирусные программы. Основные правила защиты.	опрос
5.	Тема 5. Техническая защита информации	5.1. Методы обеспечения информационной безопасности РФ. 5.2. Безопасность сетевой инфраструктуры 5.3. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. 5.4. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.	опрос

		5.5. Защита данных и резервное копирование. Аудит и мониторинг информационной безопасности	
6.	Тема 6. Цифровая гигиена	6.1. Социальная инженерия и ее предотвращение 6.2. Безопасность паролей и аутентификация. Защита личной информации в социальных сетях. Облачные хранилища: безопасность данных 6.3. Электронная почта: безопасность и конфиденциальность. 6.4. Безопасное использование мобильных устройств. 6.5. Цифровое поведение и управление временем	опрос

2.3.2 Занятия семинарского типа.

№	Наименование раздела	Примерные темы рефератов	Форма текущего контроля
1	2	3	4
1.	Тема 1	1. Основы информационной безопасности: принципы и методы защиты данных 2. Шифрование данных: современные алгоритмы и их применение 3. Информационная безопасность в корпоративной среде 4. Защита персональных данных	реферат
2.	Тема 2	1. Киберугрозы: современные тенденции и методы защиты 2. Влияние человеческого фактора на безопасность информации 3. Угрозы информации в условиях удаленной работы 4. Применение искусственного интеллекта в киберугрозах 5. Атаки на облачные хранилища данных 6. Роль шифрования в защите информации от угроз	реферат
3.	Тема 3	1. Разработка и внедрение политики безопасности информации 2. Организация работы службы информационной безопасности 3. Обучение сотрудников основам информационной безопасности 4. Правовые нормы и стандарты в области защиты информации 5. Роль руководящих работников в обеспечении безопасности информации	реферат
4.	Тема 4	1. Защита баз данных	реферат

		2. Анализ уязвимостей программного обеспечения 3. Антивирусные системы: принципы работы и виды. 4. Использование антивирусного ПО для защиты информации 5. Защита конфиденциальной информации на уровне операционной системы 6. Этические аспекты программной защиты информации	
5.	Тема 5	1. Основы технической защиты информации: понятие и принципы 2. Технологии защиты данных в облаке 3. Защита информации в корпоративной среде: стратегии и лучшие практики 4. Информационная безопасность в эпоху Интернета вещей (IoT).	реферат
6.	Тема 6	1. Фишинг и мошенничество в интернете: как распознать и избежать ловушек 2. Цифровой след: как он влияет на нашу жизнь и репутацию 3. Родительский контроль и цифровая гигиена для детей: как защитить их в интернете 4. Правовые аспекты цифровой гигиены: законы и регуляции в области защиты данных 5. Будущее цифровой гигиены: новые технологии и вызовы.	реферат

2.3.3 Лабораторные занятия.
Не предусмотрены

2.3.4 Примерная тематика курсовых работ (проектов)
Не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1.	Проработка учебного (теоретического) материала	Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. : ил., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93356 – Библиогр. в кн. – ISBN 978-5-9765-1271-9. – Текст : электронный.
2.	реферат	Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 – Библиогр.:

		с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

3. Образовательные технологии.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ООП, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе должен составлять не менее 10 процентов от общего объема аудиторных занятий.

Так как общий объем аудиторных занятий по дисциплине «Основы теории и практики защиты информации» для очной формы обучения составляет 20 часов, то занятия, проводимые в интерактивных формах, должны составлять не менее 2 часов.

Используемые интерактивные образовательные технологии по семестрам и видам занятий представлены в таблице.

Семестр	Вид занятия (Л, ПЗ, С, ЛР, КСР)	Используемые интерактивные образовательные технологии	Количество часов
В Очная форма	*Л*	«Студент в роли преподавателя»	1
	Л	«Работа в малых группах»	1
	ЛР	«Мозговой штурм»	1
	ЛР	«Творческое задание»	1
	Итого:		4

Пояснения к таблице

В современных условиях развитие продуктивных технологий в сфере образования становится неотъемлемой частью процесса модернизации. Заканчиваются возможности экстенсивного пути развития образования, при котором повышение образованности и профессиональности связывалось с увеличением объема знаний, и начинается переход к интенсивному пути развития образования. Он требует становления принципиально новых образовательных подходов в противовес широко распространенным сегодня репродуктивным технологиям, основанным на простом воспроизводстве информации. Новые технологии должны базироваться на продуктивности, креативности, мобильности и опираться на научное мышление, формирование которого у обучающихся становится основной задачей образовательного процесса.

Основные педагогические технологии

1. Традиционное обучение
2. Феноменологический подход
3. Интерактивные подходы

4. Эвристическое обучение
5. Программированное обучение
6. Контекстное обучение
7. Активное обучение
8. Дидактическая эвристика
9. Авторские педагогические технологии
10. Эмоционально-смысловой подход
11. Компьютерные технологии обучения
12. Разноуровневое обучение
13. Метод проектов
14. Учение через обучение
15. Технология парного обучения
16. Конструктивное обучение (конструктивистское обучение)
17. Нооген
18. Пренатальное обучение

Интерактивные подходы

Костяком интерактивных подходов являются интерактивные упражнения и задания, которые выполняются учащимися. Основное отличие интерактивных упражнений и заданий от обычных заключается в том, что они направлены не только и не столько на закрепление уже изученного материала, сколько на изучение нового. Современная педагогика богата целым арсеналом интерактивных подходов, среди которых можно выделить следующие:

- Творческие задания
- Работа в малых группах
- Обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры)
- Использование общественных ресурсов (приглашение специалиста, экскурсии)
- Социальные проекты и другие внеаудиторные методы обучения (социальные проекты, соревнования, радио и газеты, фильмы, спектакли, выставки, представления, песни и сказки)
- Разминки
- Изучение и закрепление нового материала (интерактивная лекция, работа с наглядными пособиями, видео- и аудиоматериалами, «ученик в роли учителя», «каждый учит каждого», мозаика (ажурная пила), использование вопросов, Сократический диалог)
- Обсуждение сложных и дискуссионных вопросов и проблем («Займи позицию (шкала мнений)», ПОПС-формула, проективные техники, «Один — вдвоем — все вместе», «Смени позицию», «Карусель», «Дискуссия в стиле телевизионного ток-шоу», дебаты, симпозиум)
- Разрешение проблем («Дерево решений», «Мозговой штурм», «Анализ казусов», «Переговоры и медиация», «Лестницы и змейки»)

Творческие задания

Под творческими заданиями мы будем понимать такие учебные задания, которые требуют от учащихся не простого воспроизводства информации, а творчества, поскольку задания содержат больший или меньший элемент неизвестности и имеют, как правило, несколько подходов. Творческое задание составляет содержание, основу любого интерактивного метода. Творческое задание (особенно практическое и близкое к жизни обучающегося) придает смысл обучению, мотивирует учащихся. Неизвестность ответа и возможность найти свое собственное «правильное» решение, основанное на своем персональном опыте и опыте своего коллеги, друга, позволяют создать фундамент для

сотрудничества, сообучения, общения всех участников образовательного процесса, включая педагога. Выбор творческого задания сам по себе является творческим заданием для педагога, поскольку требуется найти такое задание, которое отвечало бы следующим критериям:

- не имеет однозначного и односложного ответа или решения
- является практическим и полезным для учащихся
- связано с жизнью учащихся
- вызывает интерес у учащихся
- максимально служит целям обучения

Если учащиеся не привыкли работать творчески, то следует постепенно вводить сначала простые упражнения, а затем все более сложные задания.

Работа в малых группах

Работа в малых группах — это одна из самых популярных стратегий, так как она дает всем учащимся (в том числе и стеснительным) возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения (в частности, умение активно слушать, вырабатывать общее мнение, разрешать возникающие разногласия). Все это часто бывает невозможно в большом коллективе. Работа в малой группе — неотъемлемая часть многих интерактивных методов, например таких, как мозаика, дебаты, общественные слушания, почти все виды имитаций и др.

При организации групповой работы, следует обращать внимание на следующие ее аспекты. Нужно убедиться, что учащиеся обладают знаниями и умениями, необходимыми для выполнения группового задания. Нехватка знаний очень скоро даст о себе знать — учащиеся не станут прилагать усилий для выполнения задания. Надо стараться сделать свои инструкции максимально четкими. Маловероятно, что группа сможет воспринять более одной или двух, даже очень четких, инструкций за один раз, поэтому надо записывать инструкции на доске и (или) карточках. Надо предоставлять группе достаточно времени на выполнение задания.

Критическое мышление

Идея развития критического мышления является достаточно новой для российской дидактики. Заговорили о целостной технологии развития критического мышления лишь в середине 90-х годов. Но уже сегодня сторонников развития критического мышления учащихся достаточно много.

Критическое мышление означает не негативность суждений или критику, а разумное рассмотрение разнообразия подходов с тем, чтобы выносить обоснованные суждения и решения. Ориентация на критическое мышление предполагает вежливый скептицизм (ничто не принимается на веру), сомнение в общепринятых истинах, означает выработку точки зрения по определенному вопросу и способность отстоять эту точку зрения логическими доводами. Критическое мышление не является отдельным навыком, оно сочетает в себе следующие умения:

- выражать свои мысли (устно и письменно) ясно, уверенно и корректно по отношению к окружающим;
- аргументировать свою точку зрения и учитывать точки зрения других;
- брать на себя ответственность;
- работать с увеличивающимся и постоянно обновляющимся информационным потоком;
- задавать вопросы, самостоятельно формулировать гипотезу;
- решать проблемы;
- вырабатывать собственное мнение на основе осмысления различного опыта, идей и представлений;
- участвовать в совместном принятии решения;

- выстраивать конструктивные взаимоотношения с другими людьми.

Метод проектов

Основной его тезис: я знаю, для чего мне надо то, что я познаю, где и как я могу эти знания применить. Каждый обучаемый, принимая участие в проектировании, находит себе дело с учетом уровня своего интеллектуального развития, уровня подготовки по данной проблеме, своих способностей и задатков. Для того чтобы проект получился, надо верить в обучаемого. Мое твердое убеждение – нет плохих учеников. Они все яркие, талантливые, неповторимые индивидуальности.

Основные требования к использованию метода проектов:

1. Наличие значимой в исследовательском творческом плане проблемы / задачи, требующей интегрированного знания, исследовательского поиска для ее решения (например, исследование демографической проблемы в разных регионах мира; создание серии репортажей из разных концов земного шара одной проблеме и т.п.).

2. Практическая, теоретическая, познавательная значимость предполагаемых результатов. Например, доклад о демографическом состоянии данного региона, факторах, влияющих на это состояние, тенденциях, прослеживающихся в развитии данной проблемы; выпуск газеты, план мероприятий и т.п.

3. Самостоятельная (индивидуальная, парная, групповая) деятельность учащихся.

4. Использование исследовательских методов:

- определение проблемы и вытекающих из нее задач исследования;
- выдвижение гипотезы их решения;
- обсуждение методов исследования;
- обсуждение способов оформления конечных результатов (презентаций, защиты, творческих отчетов и т.п.);
- сбор, систематизация и анализ полученных данных;
- подведение итогов, оформление результатов, их презентация;
- выводы, выдвижение новых проблем исследования.

Таким образом, метод проектов является одной из самых результативных и прогрессивных педагогических технологий. Он позволяет развивать познавательные навыки учащихся, критическое мышление, умение самостоятельно конструировать свои знания, ориентироваться в информационном пространстве.

Метод «мозгового штурма»

Существуют разные формы «мозгового штурма»: групповая прямая (совместный поиск возможных решений имеющейся задачи); групповая обратная (определение недостатков в имеющейся проблеме); индивидуальная (каждый участник за короткий промежуток времени должен сформулировать не менее одной оригинальной идеи).

Перед началом «мозгового штурма» необходимо создать у обучающихся доброжелательный настрой, добиться раскованности. При проведении «мозгового штурма» возможны лишь уточняющие вопросы, абсолютно неприемлемы критические замечания и промежуточные оценки, а поощрение и поддержка партнеров приветствуется. Участники должны формулировать суждения и идеи кратко и четко, действовать по принципу «чем больше идей, решительнее атака, тем ближе достижение цели штурма».

Дискуссия

Она является одной из важнейших форм образовательной деятельности, стимулирующей инициативность учащихся. Учебный материал в ходе дискуссии усваивается за счет:

- обмена информацией между участниками;
- разных подходов к одному и тому же предмету;
- сосуществования различных, вплоть до взаимоисключающих, точек зрения;
- возможности критиковать и даже отвергать любое мнение;
- поиска группового соглашения в виде общего мнения или решения.

Задача дискуссии – коллективно, с разных точек зрения, под разными углами обсудить и исследовать спорные моменты. Основные правила ведения дискуссии:

- нельзя критиковать людей, только их идеи;
- цель дискуссии не в определении победителя, а в консенсусе;
- все участники должны быть вовлечены в дискуссию;
- выступления должны проходить организованно, с разрешения ведущего, перепалка недопустима;
- каждый участник должен иметь право и возможность высказаться;
- обсуждению подлежат все позиции; – в процессе дискуссии участники могут изменить свою позицию;
- строить аргументацию необходимо на бесспорных фактах;
- в заключение всегда должны подводиться итоги.

По ходу дискуссии преподаватель должен следить, чтобы слишком эмоциональные и разговорчивые учащиеся не подменили тему, и чтобы критика позиций друг друга была обоснованной. Соединение работы в группах с решением проблемной ситуации создает наиболее эффективные условия для обмена знаниями, идеями и мнениями, обеспечивает всесторонний анализ и обоснованный выбор решения той или иной темы. Студенты овладевают ораторскими умениями, искусством ведения полемики, что само по себе вносит важный вклад в их личностное развитие.

В целом хотелось бы отметить, что самостоятельная познавательная и мыслительная деятельность является главным средством развития личности обучающегося, она раскрывает его потенциальные способности, формирует необходимые в современном мире навыки самообразования, ориентации в стремительном потоке информации. Использование интерактивных технологий – лучший способ активизировать эту деятельность у студентов.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

По дисциплине «Информационная безопасность» предусмотрены следующие формы промежуточной аттестации: зачет в 8 семестре очной формы обучения.

Перечень вопросов для подготовки к экзамену по дисциплине «Информационная безопасность»:

1) Актуальность информационной безопасности.
2) Национальные интересы РФ в информационной сфере и их обеспечение.
3) Классификация компьютерных преступлений.
4) Способы совершения компьютерных преступлений.
5) Пользователи и злоумышленники в Интернет.
6) Причины уязвимости сети Интернет.
7) Виды угроз информационной безопасности РФ.
8) Источники угроз информационной безопасности РФ.
9) Угрозы информационной безопасности для АСОИ.
10) Удаленные атаки на интрасети.
11) Условия существования вредоносных программ.
12) Классические компьютерные вирусы.
13) Сетевые черви.
14) Троянские программы.
15) Спам.
16) Хакерские утилиты и прочие вредоносные программы.
17) Кто и почему создает вредоносные программы.
18) Признаки заражения компьютера.

19) Источники компьютерных вирусов.
20) Основные правила защиты.
21) Антивирусные программы.
22) Методы обеспечения информационной безопасности РФ.
23) Ограничение доступа.
24) Контроль доступа к аппаратуре.
25) Разграничение и контроль доступа к информации.
26) Предоставление привилегий на доступ.
27) Идентификация и установление подлинности объекта (субъекта).
28) Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
29) Методы и средства защиты информации от случайных воздействий.
30) Методы защиты информации от аварийных ситуаций.
31) Организационные мероприятия по защите информации.
32) Организация информационной безопасности компании.
33) Выбор средств информационной безопасности.
34) Информационное страхование.
35) Классификация методов криптографического закрытия информации.
36) Симметричные криптосистемы.
37) Криптосистемы с открытым ключом (асимметричные).
38) Характеристики существующих шифров.
39) Кодирование.
40) Стеганография.
41) Электронная цифровая подпись.
42) Законодательство в области лицензирования и сертификации.
43) Правила функционирования системы лицензирования.
44) Критерии безопасности компьютерных систем. «Оранжевая книга».
45) Руководящие документы Гостехкомиссии.

Тематика практических заданий на экзамене:

1) Профилактика компьютерных систем от заражения вирусами.
2) Защита информации с помощью пароля.
3) Исследование средств безопасности операционных систем.
4) Аутентификация пользователей Web-систем средствами технологии PHP.
5) Защита баз данных.
6) Исследование метода компьютерной стеганографии для защиты информации.
7) Разработка и реализация алгоритма криптографического преобразования.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029

3. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542739

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1) Информационные системы и технологии : научно-технический журнал / ред. сов. В.А. Голенков ; редкол. О.П. Архипов ; гл. ред. И.С. Константинов ; учред. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Государственный университет — учебно-научно-производственный комплекс» (Госуниверситет – УНПК) - Орел : Госуниверситет - УНПК, 2012. - № 5(73). - 152 с.: ил. - ISSN 2072-8964 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=321622

2) Фефилов, А.Д. Методы и средства защиты информации в сетях / А.Д. Фефилов. - Москва : Лаборатория книги, 2011. - 105 с. : ил., табл. - ISBN 978-5-504-00608-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=140796

3) Голиков, А.М. Основы проектирования защищенных телекоммуникационных систем: курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации. - Томск : ТУСУР, 2016. - 396 с. : ил.,табл., схем. - (Учебная литература для вузов). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480796

4) Информационные технологии : учебное пособие / сост. К.А. Катков, И.П. Хвостова, В.И. Лебедев, Е.Н. Косова и др. - Ставрополь : СКФУ, 2014. - Ч. 1. - 254 с. : ил. -

Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457340

5.3. Периодические издания:

№ п/п	Название издания	Периодичность выхода (в год)	За какие годы хранится	Место хранения	Срок хранения
1.	Инфокоммуникационные технологии	4	2006; 2008-	чз	5 лет
2.	Информатика и образование	6	1992-	чз	пост.
3.	Информатика. Реферативный журнал ВИНИТИ	12	1987-	зал РЖ	пост.
4.	Информационное общество		2006-	чз	5 лет
5.	Информационные ресурсы России	6	2007 с №4-	чз	5 лет
6.	Информационные технологии	12	1996-	чз	пост.
7.	Мир компьютерной автоматизации - Мир встраиваемых компьютерных технологий	4	2006-	чз	5 лет
8.	Мир ПК	12	2006-2009	чз	5 лет
9.	Нейрокомпьютеры: разработка, применение	12	2004-	чз	10 лет
10.	Открытые системы. СУБД	12	2005-	чз	
11.	Прикладная информатика	6	2007 с №4-	чз	пост.
12.	Проблемы передачи информации	4	2005-	чз	пост.
13.	Программирование	6	1975-	чз	пост.
14.	Программные продукты и системы		2005-	чз	пост.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

№ п/п	Ссылка	Пояснение
1.	http://www.book.ru	BOOK.ru – электронная библиотечная система (ЭБС) современной учебной и научной литературы. Библиотека BOOK.ru содержит актуальную литературу по всем отраслям знаний, коллекция пополняется электронными книгами раньше издания печатной версии.
2.	http://www.ibooks.ru	Айбукс.ру – электронная библиотечная система учебной и научной литературы. В электронную коллекцию включены современные учебники и пособия ведущих издательств России.
3.	http://www.sciencedirect.com	Платформа ScienceDirect обеспечивает всесторонний охват литературы из всех областей науки, предоставляя доступ к более чем 2500 наименований журналов и более 11000 книг из коллекции издательства «Эльзевир», а также огромному числу журналов, опубликованных

		престижными научными сообществами. Полнотекстовая база данных ScienceDirect является непревзойденным Интернет-ресурсом научно-технической и медицинской информации и содержит 25% мирового рынка научных публикаций.
4.	http://www.scopus.com	База данных Scopus индексирует более 18 тыс. наименований журналов от 5 тыс. международных издательств, включая более 300 российских журналов. Непревзойденная поддержка в поиске научных публикаций и предоставлении ссылок на все вышедшие рефераты из обширного объема доступных статей. Возможность получения информации о том, сколько раз ссылались другие авторы на интересующую Вас статью, предоставляется список этих статей. Отслеживание своих публикаций с помощью авторских профилей, а так же работы своих соавторов и соперников.
5.	http://www.scirus.com	Scirus – бесплатная поисковая система для поиска научной информации.
6.	http://www.elibrary.ru	Научная электронная библиотека (НЭБ) содержит полнотекстовые версии научных изданий ведущих зарубежных и отечественных издательств.
7.	http://scitation.aip.org	Базы данных Американского института физики American Institute of Physics (AIP).Тематика баз данных: физика (в т.ч. оптика, акустика, ядерная физика, математическая физика), механика (техническая механика), астрономия, химия и химическая техноло-гия, биоинженерия, энергетика, электроника, вычислительная техника (применение компьютеров в науке и технике), приборостроение, строительство. Список доступных полнотекстовых журналов: Applied Physics Letters (2001-2006) Chaos (1991-2006) J. of Applied Physics (2001-2006) J. of Chemical Physics (2001-2006) J. of Mathematical Physics (2001-2006) Journal of Physical and Chemical Reference Data (1999 -2006) Low Temperature Physics (1997 -2006) Physics of Fluids (2001-2006) Physics of Plasmas (2001-2006) Review of Scientific Instruments (2001-2006)
8.	http://diss.rsl.ru	«Электронная библиотека диссертаций» Российской Государственной Библиотеки (РГБ) в настоящее время содержит более 400 000 полных текстов наиболее часто запрашиваемых читателями диссертаций. Ежегодное оцифровывание от 25000 до 30000 диссертаций.
9.	http://www.lektorium.tv	«Лекториум ТВ» – видеолекции ведущих лекторов России. Лекториум – on-line – библиотека, где ВУЗы и известные лектории России презентуют своих лучших лекторов. Доступ к материалам свободный и бесплатный. Все видеозаписи публикуются только на основании договоров.
10.	http://moodle.kubsu.ru	Среда модульного динамического обучения
11.	http://mschool.kubsu.ru	Библиотека информационных ресурсов кафедры информационных образовательных технологий

7. Методические указания для обучающихся по освоению дисциплины (модуля).

Основными формами аудиторных занятий по дисциплине «Информационная безопасность» для очной и заочной формы обучения являются лекции и семинары.

Лекции по дисциплине «Информационная безопасность» следует проводить в компьютерных классах кафедры теоретической физики и компьютерных технологий с использованием средств мультимедиа. При подготовке отдельных вопросов лекций или лекций по определенным темам учебной программы рекомендуется активно привлекать студентов, реализуя такие виды интерактивных образовательных технологий, как «Студент в роли преподавателя» и «Работа в малых группах».

Практические занятия по дисциплине «Информационная безопасность» следует проводить в компьютерных классах кафедры теоретической физики и компьютерных технологий. Выполнение лабораторных работ сочетает различные виды практических заданий и упражнений. На лабораторных работах рекомендуется использовать образовательные технологии «Мозговой штурм» и «Творческое задание». При выполнении работ используются локальные и глобальные сети.

Структура дисциплины «Информационная безопасность» для очной и заочной формы обучения определяет следующие виды самостоятельной работы: самостоятельная работа студента (СРС).

Самостоятельная работа студента является основным видом самостоятельной работы. Она проводится в целях закрепления знаний, полученных на всех видах учебных занятий, а также расширения и углубления знаний, т.е. активного приобретения студентами новых знаний.

СРС включает проработку и повторение лекционного материала. Для этого студенту рекомендуется прочитать текст лекции, пересказать его вслух, воспроизвести самостоятельно имеющиеся в тексте структурно-логические схемы, диаграммы, математические выкладки формул, доказательства теорем и т.п. Проработку лекционного материала следует проводить сначала последовательно, по каждому учебному вопросу, а затем повторно, по всему тексту лекции.

СРС также включает изучение материала по рекомендованным учебникам и учебным пособиям. Так как существует огромное количество учебной литературы, то для этого вида подготовки необходимо предварительное указание преподавателя. Преподаватель должен выступать здесь в роли опытного «путеводителя», определяя последовательность знакомства с литературными источниками и «глубину погружения» в каждый из них.

Одним из видов СРС является подготовка к лабораторным работам. Преподаватель накануне очередного занятия обозначает для студентов круг теоретического материала, необходимого для выполнения лабораторной работы. Студенты прорабатывают его. Затем, уже в аудитории, перед выполнением заданий, преподаватель производит контрольный опрос студентов. Это позволяет определить степень готовности группы по данной теме и скорректировать ход занятия.

Преподаватель должен прогнозировать затруднения, которые могут возникнуть у студентов при самостоятельном изучении и усвоении учебного материала и предусмотреть оперативную консультацию по любому вопросу. Если возникают затруднения по одному и тому же материалу (вопросу) у многих студентов, то желательно провести групповую консультацию. Консультации должны быть краткими: групповая - 2-3 мин., индивидуальная - 1-2 мин. Глубину и качество усвоения учебного материала необходимо непрерывно отслеживать при проведении текущего контроля знаний.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

1) Использование электронных презентаций при проведении лекций.
2) Подготовка к тестированию и консультирование посредством электронной почты.

8.2 Перечень необходимого программного обеспечения.

1) Растровый графический редактор Paint Операционная система Windows
2) Программа разработки презентаций Microsoft PowerPoint Дистрибутив Microsoft Office
3) Электронные таблицы Microsoft Excel Дистрибутив Microsoft Office
4) Текстовый процессор Microsoft Word Дистрибутив Microsoft Office
5) Компиляторы Basic, Pascal, C++
6) Система математических вычислений MathCAD
7) Система математических вычислений MatLAB

8.3 Перечень информационных справочных систем:

Не предусмотрены

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Учебные аудитории для проведения лекционных занятий – ауд. 213, корп. С, вычислительный центр (ул. Ставропольская, 149)
2.	Семинарские занятия	Учебные аудитории для проведения семинарских занятий– ауд. 213, корп. С, вычислительный центр (ул. Ставропольская, 149)
3.	Самостоятельная работа	Аудитория для самостоятельной работы – ауд. 208, корп. С (ул. Ставропольская, 149)