МИНИСТЕРСТВО НАУКИ и ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет Информатики и Информационных Технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технологии обеспечения информационной безопасности

Кафедра информационных систем и технологий программирования

Образовательная программа
09.04.03 - Прикладная информатика

Профиль подготовки:
Разработка и внедрение информационных систем

Уровень высшего образования:
магистратура

Форма обучения
очная

Статус дисциплины:
входит в часть ОПОП, формируемую участниками образовательных отношений

Махачкала, 2021

Рабочая программа дисциплины «Технологии обеспечения информационно безопасности» составлена в 2021г в соответствии с требованиями ФГОС ВО - магистратура по направлению подготовки 09.04.03 - Прикладная информатика от 19 сентября 2017 г. N 916

Составитель: Ахмедова З.Х, доцент каф. ИТиБКС

Рабочая программа дисциплины одобрена:
на заседании кафедры ИСиТП от «29» июня 2021г., протокол № 11
Зав. кафедрой _____ Исмиханов З.Н.
(подпись)

на заседании Методической комиссии факультета ИиИТ
от «29» июня 2021г., протокол № 11.

Председатель _____ Бакмаев А.Ш.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «9» июля 2021г.

Начальник УМУ _____ Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Технологии обеспечения информационно безопасности» входит в часть ОПОП, формируемую участниками образовательной программы магистратура по направлению 09.04.03 - Прикладная информатика

Дисциплина реализуется на факультете информатики и информационных технологий кафедрой ИТиБКС.

Дисциплина нацелена на формирование следующих компетенций выпускника: ОПК-8; ПК-3; Пк-5.

Содержание дисциплины охватывает круг вопросов, связанных с изучением содержания и основных составляющих компьютерной безопасности, структуры и задач органов, обеспечивающих информационную безопасность, а также с анализом методов обеспечения компьютерной безопасности РФ.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, лабораторные занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости: формы контроля текущей успеваемости: коллоквиум, контрольная работа, тестирование, форма промежуточного контроля: зачет.

Объем дисциплины 4 зачетных единиц, в том числе в академических часах по видам учебных занятий

Объем дисциплины в очной форме

Семестр	Всего	Учебные занятия					Форма промежуточной аттестации
		в том числе					
		Контактная работа обучающихся с преподавателем				СРС, в том числе экзамен	
		Всего	из них				
			Лекции	Лабораторные занятия	Практические занятия		
4	144	48	16	16	16	96	зачет

1.Цели освоения дисциплины

Формирование представления о специфике дисциплины, об основных составляющих компьютерной безопасности; о проблемах и методах их исследования Изучение методов и средств управления информационной безопасностью на определенном объекте

Введение в круг гуманитарных проблем, связанных с областью профессиональной деятельности

Выработка навыков анализа угроз компьютерной безопасности

2. Место дисциплины в структуре ОПОП магистратцры.

Дисциплина входит в часть ОПОП, формируемую участниками образовательной программы магистратуры по направлению **09.04.03 - Прикладная информатика.**

3.Компетенции обучающего, формируемые в результате освоения дисциплины.

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

Код и наименование компетенции из ОПОП	Код и наименование индикатора достижения	Планируемые результаты обучения	Процедура освоения
ОПК-8 Способен осуществлять эффективное управление разработкой программных средств и проектов	ОПК-8.1. Знать архитектуру информационных систем предприятий и организаций; методологии и технологии реинжиниринга, проектирования и аудита прикладных информационных систем различных классов; инструментальные средства поддержки технологии проектирования и аудита информационных систем и сервисов; методы оценки экономической эффективности и качества, управления надежностью и информационной безопасностью; особенности процессного подхода к управлению прикладными ИС;	Знает: архитектуру информационных систем предприятий и организаций; методологии и технологии реинжиниринга, проектирования и аудита прикладных информационных систем различных классов; инструментальные средства поддержки технологии проектирования и аудита информационных систем и сервисов; методы оценки экономической эффективности и качества, управления надежностью и информационной безопасностью; особенности процессного подхода к управлению прикладными ИС; современные ИКТ в процессном управлении; системы управления качеством; концептуальное моделирование процессов управления знаниями; архитектуру систем управления знаниями; онтологии знаний; подсистемы сбора, фильтрации, накопления, доступа,	Устный опрос, письменный опрос

	современные ИКТ в процессном управлении; системы управления качеством; концептуальное моделирование процессов управления знаниями; архитектуру систем управления знаниями; онтологии знаний; подсистемы сбора, фильтрации, накопления, доступа, генерации и распространения знаний;	генерации и распространения знаний; Умеет: выбирать методологию и технологию проектирования информационных систем; обосновывать архитектуру ИС; управлять проектами ИС на всех стадиях жизненного цикла, оценивать эффективность и качество проекта; применять современные методы управления проектами и сервисами ИС; использовать инновационные подходы к проектированию ИС; принимать решения по информатизации предприятий в условиях неопределенности; проводить реинжиниринг прикладных и информационных процессов; обосновывать архитектуру системы правления знаниями;	
ПК-3. Способность проектировать информационные процессы и системы с использованием инновационных инструментальных средств	ПК-3.1. Знать: устройство и функционирование современных ИС; методы анализа прикладной области, методологии и технологии проектирования ИС; инновационные методы и инструментальных средства проектирования информационных процессов и систем. ПК-3.2. Уметь: проектировать информационные процессы и системы, адаптировать современные ИКТ ПК-3.3. Владеть: способностью проектировать информационные процессы и системы с использованием инновационных методов и инструментальных	Знает: устройство и функционирование современных ИС; методы анализа прикладной области, методологии и технологии проектирования ИС; инновационные методы и инструментальных средства проектирования информационных процессов и систем Умеет: проектировать информационные процессы и системы, адаптировать современными ИКТ. Владеет: способностью проектировать информационные процессы и системы с использованием инновационных методов и инструментальных средств, адаптировать современные ИКТ к задачам прикладных:	Устный опрос, письменный опрос

	средств, адаптировать современные ИКТ к задачам прикладных ИС		
ПК-5. Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	ПК-5.1. Знать: передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС ПК-5.2. Уметь: использовать передовые методы оценки качества, надежности и информационной безопасности ИС ПК-5.3. Владеть: передовыми методами оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	Знает: передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС Умеет: использовать передовые методы оценки качества, надежности и информационной безопасности ИС Владеет: передовыми методами оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	письменный опрос

4. Объем, структура и содержание дисциплины.

4.1.Объем дисциплины.

Объем дисциплины составляет 4 зачетные единицы, 144 академических часа.

4.2. Структура дисциплины

4.2.1. Объем дисциплины в очной форме.

№ п/п	Раздел дисциплины	Семестр	Неделя семестр[a]	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости (по неделям семестра). Формы промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
	I модуль. Место и роль проблем компьютерной безопасности в становлении современного информационного общества							
1.	Понятие и составляющие компьютерной безопасности			2			4	Устный опрос
2.	Нормативные документы в области компьютерной безопасности				4	2	16	Устный опрос
3	Гуманитарная сущность компьютерной безопасности			2		2	4	тестирование
	Итого за модуль			4	4	4	24	
	II модуль. Проблемы обеспечения баланса интересов личности, общества и государства в информационной сфере							
	Обеспечение информационно-психологической безопасности личности и общества			4	2		10	тестирование
	Компьютерные правонарушения			2		2	8	Письменная работа

6	Структура и задачи органов, обеспечивающих информационную безопасность			2	2	2	6	Письменная работа
	Итого за модуль			4	4	4	24	
	III модуль. Ценностная ориентация личности, ее информационное обоснование и информационная безопасность2							
7	Проблемы свободы слова			2	2	2	12	Контрольная работа
8	Информационное пространство и проблема целостности российского государства			2	2	2	12	Устный опрос
	Итого за модуль			4	4	4	24	
	IV модуль. Обеспечение информационно-психологической безопасности личности и общества							
9	Нормативные документы в области компьютерной безопасности			2	2	2	10	Контрольная работа
10	Место и роль проблем компьютерной безопасности в становлении современного информационного общества			2	2	2	12	Устный опрос
	Итого за модуль			4	4	4	24	
	ИТОГО	**144**		**16**	**16**	**16**	**96**	зачет

4.3.1. Содержание лекционных занятий по дисциплине

Модуль 1. **Место и роль проблем компьютерной безопасности в становлении современного информационного общества**

Тема 1. Понятие, содержание и основные составляющие компьютерной безопасности

Использование естественно возникавших средств информационных коммуникаций.

Защита сведений, имеющих для человека жизненное значение. Использование искусственно создаваемых технических средств радиосвязи.

Появление радиолокационных и гидроакустических средств. Сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств. Изобретение и внедрение в практическую деятельность электронно-вычислительных машин.

Создание и развитие локальных информационно-коммуникационных сетей.

Использование сверхмобильных коммуникационных устройств с широким спектром задач. Создание и развитие глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения.

Отличительные черты информационного общества. Основные этапы развития средств информационных коммуникаций. Составляющие информационной сферы современного социума.

Сущность понятий «информация», «информационная безопасность», «информационная безопасность государства», «поддерживающая инфраструктура компьютерной безопасности». Потребители и обладатели (производители) информации.

Основные тенденции в органах государственной власти в определении понятия и структуры компьютерной безопасности.

Объекты компьютерной безопасности: сознание, психика людей; информационно-технические системы различного масштаба и назначения. Субъекты компьютерной безопасности - органы и структуры, обеспечивающие информационную безопасность. Средства обеспечения компьютерной безопасности - средства, с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации. Основные категории модели компьютерной безопасности: конфиденциальность, целостность, доступность. Теоретико-методологические основы компьютерной безопасности.

Тема 2. Нормативные документы в области обеспечения компьютерной безопасности

Основные нормативно-правовые акты в области защиты информации. Общие нормативные правовые акты по вопросам защиты информации ограниченного доступа, не содержащей государственной тайны, по вопросам безопасности информационных систем персональных данных. Информационные письма (сообщения). Информационные письма по вопросам электронной цифровой подписи. Сопутствующие нормативные правовые акты по безопасности информации: организационно-распорядительные документы, специальные нормативные документы, государственные стандарты

Тема 3. Структура и задачи органов, обеспечивающих информационную безопасность

Органы (подразделения), обеспечивающие информационную безопасность: Комитет ГД по безопасности; Совет безопасности РФ; Федеральная служба по техническому и экспертному контролю (ФСТЭК России); Федеральная служба безопасности РФ (ФСБ России); Федеральная служба охраны РФ (ФСО России); Служба внешней разведки РФ (СВР России); Министерство обороны РФ (Минобороны России); Министерствовнутренних дел РФ (МВД России); Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Службы, организующие защиту информации на уровне предприятия: Служба экономической безопасности; Служба безопасности персонала (Режимный отдел); Отдел кадров; Служба компьютерной безопасности.

Структура государственных органов, обеспечивающих информационную безопасность: Основные направления защиты информационной системы: защита объектов информационной системы; защита процессов, процедур и программ обработки информации; защита каналов связи, подавление побочных электромагнитных излучений; управление системой защиты.

Программно - технические способы и средства обеспечения компьютерной безопасности: Средства защиты от несанкционированного доступа (НСД); средства авторизации; Мандатное управление доступом; Избирательное управление доступом; Управление доступом на основе ролей; Журналирование (Аудит). Системы мониторинга сетей: Системы обнаружения и предотвращения вторжений; Системы предотвращения утечек конфиденциальной информации; Анализаторы протоколов; Межсетевые экраны.

Модуль 2. Информационная безопасность РФ

Тема 1. Национальные интересы РФ в информационной сфере и их обеспечение

Основные составляющие национальных интересов РФ в информационной сфере: соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России; информационное обеспечение государственной политики РФ, связанное с доведением до общественности достоверной информации о государственной политике РФ; развитие современных информационных технологий, отечественной индустрии информации; развитие микроэлектронной и компьютерной промышленности; защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Тема 2. Виды и источники угроз компьютерной безопасности РФ

Угрозы компьютерной безопасности РФ: угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности; угрозы информационному обеспечению государственной политики РФ; угрозы развитию отечественной индустрии информации; угрозы безопасности информационных и телекоммуникационных средств и систем.

Внешние источники угроз компьютерной безопасности РФ: деятельность иностранных разведывательных и информационных структур; обострение международной конкуренции за обладание информационными технологиями; деятельность международных террористических организаций; разработка концепций информационных войн.

Внутренние источники угроз компьютерной безопасности РФ: критическое состояние отечественных отраслей промышленности; недостаточная координация деятельности органов государственной власти; недостаточная разработанность нормативной правовой базы; неразвитость институтов гражданского общества; недостаточная экономическая мощь государства; снижение эффективности системы образования и воспитания; отставание России от ведущих стран по уровню информатизации федеральных органов государственной власти.

Общие методы обеспечения компьютерной безопасности РФ: правовые, организационно-технические и экономические.

Правовые методы обеспечения компьютерной безопасности РФ: разработка нормативных правовых актов, регламентирующих отношения в информационной сфере; разграничение полномочий в области обеспечения компьютерной безопасности РФ между федеральными органами государственной власти и органами государственной власти субъектов РФ.

Организационно-технические методы обеспечения компьютерной безопасности РФ: создание и совершенствование системы обеспечения компьютерной безопасности РФ; выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем; сертификация средств защиты информации; контроль действий персонала в защищенных информационных системах.

Экономические меры обеспечения компьютерной безопасности РФ (разработка программы обеспечения компьютерной безопасности РФ и определение порядка ее финансирования; совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц).

Тема 3. Основные направления государственной политики обеспечения компьютерной безопасности РФ в различных сферах общественной жизни

Общие и частные методы обеспечения компьютерной безопасности в различных сферах общественной жизни.

Обеспечение компьютерной безопасности РФ в сфере экономики как важнейшее направление обеспечения национальной безопасности РФ. Наиболее важные объекты и основные мероприятия по обеспечению компьютерной безопасности РФ в сфере внутренней политики. Объекты и основные мероприятия по обеспечению компьютерной безопасности РФ в сфере внешней политики. Основные объекты обеспечения компьютерной безопасности РФ в области науки и техники. Основные внешние и внутренние угрозы компьютерной безопасности РФ в области науки и техники. Мероприятия по обеспечению компьютерной безопасности РФ в области науки и техники. Основные направления обеспечения компьютерной безопасности РФ в сфере духовной жизни. Объекты обеспечения компьютерной безопасности РФ в общегосударственных информационных и телекоммуникационных системах. Основные организационно-технические мероприятия по защите информации в общегосударственных и телекоммуникационных системах. Объекты обеспечения компьютерной безопасности РФ в сфере обороны. Внешние и внутренние угрозы для объектов обеспечения компьютерной безопасности РФ в сфере обороны. Главные направления совершенствования системы обеспечения компьютерной безопасности РФ в сфере обороны. Объекты обеспечения компьютерной безопасности РФ в правоохранительной сфере и судебной сфере. Внешние и внутренние угрозы для объектов обеспечения компьютерной безопасности РФ в правоохранительной сфере и судебной сфере.

Наиболее уязвимые объекты обеспечения компьютерной безопасности РФ в условиях чрезвычайных ситуаций. Специфические для данных условий направления обеспечения компьютерной безопасности.
Основные принципы государственной политики обеспечения компьютерной безопасности РФ. Направления деятельности государства в процессе реализации его функций по обеспечению компьютерной безопасности РФ. Первоочередные мероприятия по реализации государственной политики обеспечения компьютерной безопасности РФ. Основные группы научных проблем обеспечения компьютерной безопасности РФ. Пути решения гуманитарных, научно-технических проблем и проблем кадрового обеспечения компьютерной безопасности РФ.
4.3.2. Содержание лабораторно-практических занятий по дисциплине.
Модуль 1.
Основы системного понимания компьютерной безопасности
Тема 1. Понятие, содержание и основные составляющие компьютерной безопасности
Сущность и основные этапы развития средств информационных коммуникаций 2.Объекты и субъекты компьютерной безопасности
3.Средства и методы обеспечения компьютерной безопасности
Тема 2. Нормативные документы в области компьютерной безопасности
1.Основные нормативно - правовые документы в области защиты информации.
Сопутствующие и специальные документы в области защиты информации
Тема 3. Структура и задачи органов, обеспечивающих информационную безопасность
Структура государственных органов, обеспечивающих информационную безопасность
Службы, организующие защиту информации на уровне предприятия
3.Организационно-технические и режимные меры и методы обеспечения компьютерной безопасности
Модуль 2. Информационная безопасность РФ
Тема 1. Национальные интересы РФ в информационной сфере и их обеспечение
1.Доктрина компьютерной безопасности РФ
2.Основные составляющие национальных интересов РФ в информационной сфере Тема 2. Источники угроз и методы обеспечения компьютерной безопасности РФ
Внешние и внутренние источники угроз компьютерной безопасности РФ
Правовые методы и экономические меры обеспечения компьютерной безопасности РФ
3.Организационно - технические методы обеспечения компьютерной безопасности РФ Тема 3. Особенности и основные направления государственной политики обеспечения компьютерной безопасности РФ в различных сферах общественной жизни
1.Основные меры по обеспечению компьютерной безопасности РФ в сфере экономики и политики, в сфере духовной жизни
2.Организационно - технические мероприятия по защите информации в общегосударственных информационных и телекоммуникационных системах 3 .Главные направления совершенствования системы обеспечения компьютерной безопасности РФ в сфере обороны
4.Основные группы научных и гуманитарных проблем обеспечения безопасности РФ 5.Образовательные технологии
При реализации различных видов учебной работы предусматриваются следующие образовательные технологии:
-традиционные и интерактивные лекции;
-семинары и коллоквиумы;
-подготовка доклада, творческого эссе;
-участие в научно-методологических семинарах, коллоквиумах и конференциях; -консультации преподавателя;
-встречи с представителями государственных и общественных организаций, -мастер-классы экспертов и специалистов;
-самостоятельная работа, подготовка к семинарским занятиям с использованием интернета и электронных библиотек, выполнение письменных работ

5.Образовательные технологии.

Весь курс разбит на две части. В рамках лекционных занятий (Темы 1– 4) проводится знакомство студентов с терминологией дисциплины, дается необходимая теоретическая информация, касающаяся вопросов организации облачной инфраструктуры, требований к техническому и программному обеспечению, требований к безопасности. В рамках практических занятий (Тема 5) студенты знакомятся с главами дисциплины, лежащими в основе практических навыков администрирования облачных приложений и

облачного программирования. Как лекционные, так и практические занятия проводятся в интерактивной форме, предполагающей активное участие студента в обсуждении вопросов дисциплины. Для подачи материала используются мультимедийные презентации. Текущий контроль успеваемости проводится в виде тестирования. Для усвоения практических навыков студентам предлагается выполнить ряд заданий самостоятельно. В рамках курса планируется использование средств порталов eor.dgu.ru для интерактивного общения студентов и преподавателя в рамках самостоятельной работы и для проведения учета текущей успеваемости студентов. К образовательному процессу планируется подключение ведущих специалистов компании «Мирантис ИТ». При обучении лиц с ограниченными возможностями и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве; увеличивается время на самостоятельное освоение материала.

6.Учебно-методическое обеспечение самостоятельной работы студентов обучающихся по дисциплине.

Форма контроля и критерий оценок

В соответствии с учебным планом предусмотрен экзамен в четвертом семестре.
Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине предполагают следующее распределение баллов.
Текущий контроль

- Выполнение 1 домашней работы 10 баллов
- Активность в системе Moodle - 60 баллов

Примерное распределение времени самостоятельной работы студентов

Вид самостоятельной работы	Примерная трудоёмкость, а.ч.	Примерная трудоёмкость, а.ч.	Формируемые компетенции
	Очная	Очно-заочная	
Текущая СРС			
работа с лекционным материалом, с учебной литературой	10	-	ОПК-8
опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	10	-	ОПК-5
самостоятельное изучение разделов дисциплины	10	-	ОПК-8
выполнение домашних заданий, домашних контрольных работ	10		ПК-3
подготовка к лабораторным работам, к практическим и семинарским занятиям	36		ОПК-8, ПК-3
подготовка к контрольным работам, коллоквиумам, зачётам	10		ПК-3
подготовка к экзамену (зачету)			ОПК-8, ПК-3
Творческая проблемно-ориентированная СРС			
поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме		-	
исследовательская работа, участие в конференциях, семинарах, олимпиадах		-	
анализ данных по заданной теме, написание программ, составление моделей на основе исходных данных	10	-	ПК-3
ИТОГО:	96 ч	-	

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

7.1. Типовые контрольные задания или иные материалы

Б) Примерные тестовые задания
В современном мире информация - это
а) социальный институт
б) производительная сила
в) источник опасности
г) научная теория
В условиях информатизации общества особую ценность обретают
а) этнические общности
б) национальные группы
в) новые технологии
г) люди - носители знаний
Современные информационные технологии формируют информационное единство
а) эпохи
б) культуры
в) цивилизации
г) формации
С точки зрения обладателя, сохранение в тайне важной информации позволяет успешно конкурировать
а) на рынке производства детских игрушек
б) в сфере предоставления компьютерных услуг
в) в сфере потребления товаров и услуг
г) на рынке производства и сбыта товаров и услуг
Уровень информационного обеспечения труда ученых, инженеров влияет на научно-технический потенциал
а) государства
б) партии
в) организации
г) этноса
Информационному обеспечению различных сторон современного общества способствовала
а) обработка информации
б) дифференциация технологий
в) системная классификация информации
г) деятельность политиков
Объекты компьютерной безопасности
а) информационно-технические системы и психика людей
б) компьютерные технологии и технические средства
в) средства массовой информации и телевидение
г) военная техника и инфраструктура Субъекты компьютерной безопасности
а) экономические структуры
б) политические институты
в) специальные органы и структуры
г) специальные подразделения
Естественные источники информационных опасностей
а) случайные факторы
б) специальные программы в) ценная информация г) компьютерные сети
Умышленные источники информационных опасностей
а) непреднамеренные ошибки
б) стихийные бедствия
в) компьютерные сети
г) радиолокационная борьба
Социальные преступления, основанные на использовании современной информационной технологии
а) управление поведением людей
б) негативное воздействие на психику людей
в) махинации с электронными деньгами
г) воздействие на компьютерные системы
Основная тенденция современного общественного развития - рост воздействия СМИ на содержание
а) национальных отношений
б) информационных технологий в) экономической ситуации г) политических процессов

Информационная безопасность - это важнейший аспект
а) интегральной безопасности
б) экономической безопасности
в) политической безопасности
г) национальной безопасности Внедрение ценной информации способствует
а) снижению качества используемой информации
б) усилению влияния лидера в социальной группе
в) повышению эффективности деятельности субъекта
г) повышению рейтинга политической партии
Защищенность национальных интересов в информационной сфере - обязательное условие обеспечения
а) компьютерной безопасности государства
б) национальной политики общества
в) информатизации всех структур общества
г) компьютерной безопасности государства Стандартная модель безопасности состоит из трех категорий
а) достоверность, доступность, целостность
б) целостность, системность, доступность
в) конфиденциальность, системность, целостность
г) конфиденциальность, целостность, доступность Нормативно-правовые акты в области компьютерной безопасности
а) Указы Президента РФ
б) Рекомендация Правительства РФ
в) Методические указания ученых
г) Перспективы развития РФ
Доктрина Компьютерной безопасности РФ утверждена
а) 25 июня 2005 года
б) 21 декабря 2001 года
в) 5 августа 2009 года
г) 9 сентября 2000 года
Федеральный закон «Об информации, информационных технологиях и о защите информации» принят
а) 27 июля 2006 года
б) 30 марта 2007 года
в) 10 марта 2008 года
г) 1 августа 2009 года
Методы обеспечения компьютерной безопасности РФ в Доктрине ИБ РФ
а) правовые, организационно-технические, экономические
б) социально-политические, духовные, экономические
в) культурно-информационные, технические, социальные
г) организационно-технические, экономические, духовные
В) Контрольные вопросы и задания для текущего контроля и промежуточной аттестации.

Типовые контрольные задания
А) *Тематика рефератов, докладов, эссе, научных сообщений Тематика рефератов*
Отличительные черты информационного общества
Информационное общество тотального риска
Потребители и обладатели (производители) информации
Теоретико-методологические основы компьютерной безопасности.
5.Основные функции системы обеспечения компьютерной безопасности 6.Основные концептуальные проблемы информатизации
Конфиденциальность, целостность и доступность как основные категории модели компьютерной безопасности
Информационная технология: понятие и виды
Использование информационных технологий в современном обществе
Гуманитарные проблемы обеспечения компьютерной безопасности
Доктрина компьютерной безопасности Российской Федерации 12.Основные принципы государственной политики обеспечения компьютерной безопасности РФ
Проблемы кадрового обеспечения компьютерной безопасности РФ

Правовое обеспечение компьютерной безопасности
Научно - технические проблемы обеспечения компьютерной безопасности РФ 16.Организационная основа системы обеспечения компьютерной безопасности РФ
Национально-государственная безопасность Российской Федерации
Военная безопасность Российской Федерации
Специфика обеспечения компьютерной безопасности РФ в условиях чрезвычайных ситуаций
Системы менеджмента компьютерной безопасности

Примерный перечень вопросов к зачету

Исторические аспекты возникновения и развития компьютерной безопасности 2.Основные составляющие компьютерной безопасности
Источники информационных опасностей
Информатизация и проблемы компьютерной безопасности 5.Основные категории модели компьютерной безопасности 6.Обеспечение компьютерной безопасности: содержание и структура понятия
7. Информация, защищаемая информация, объект информатизации, информационные ресурсы, информационная технология
8.Защита информации. Основные термины и определения
9.Основные нормативно - правовые акты в области защиты информации
10.Специальные нормативные документы и государственные стандарты
11.Структура государственных органов, обеспечивающих информационную безопасность
12.Национальные интересы РФ в информационной сфере и их обеспечение
13.Внешние источники компьютерной безопасности РФ
14.Внутренние источники компьютерной безопасности РФ
15.Общие методы обеспечения компьютерной безопасности РФ
16.Правовые и организационно - технические методы обеспечения компьютерной безопасности РФ
17.Особенности обеспечения компьютерной безопасности РФ в сфере экономики
18.Специфика обеспечения компьютерной безопасности РФ в сфере внешней политики
19.Проблемы обеспечения компьютерной безопасности РФ в области науки и техники
20.Основные направления обеспечения ИБ РФ в сфере духовной жизни
21.Главные направления совершенствования системы обеспечения ИБ РФ в сфере обороны
22.Основные направления совершенствования системы обеспечения ИБ РФ в правоохранительной сфере
23.Особенности обеспечения компьютерной безопасности РФ в условиях чрезвычайных ситуаций
24.Основные группы научных проблем обеспечения компьютерной безопасности РФ
25.Анализ рисков компьютерной безопасности: основные подходы, основные этапы процесса

Учебно-методическое обеспечение самостоятельной работы студентов

Основными видами самостоятельной работы студентов являются:
-работа с учебной и справочной литературой;
-конспектирование первоисточников;
-выполнение индивидуальных домашних заданий, задач и упражнений;
-изучение научной литературы по отдельным темам курса;
-подготовка рефератов, научных сообщений по темам;
-подготовка докладов к научным конференциям
Материалы для подготовки к самостоятельной работе студентов, представленные на сайте кафедры философии и социально-политических наук:
Перечень основной, словарно-справочной и дополнительной литературы. Режим доступа: http://cathedra.icc.dgu.ru/Informati on.aspx?Value=8&id=1479
Индивидуальные задания, задачи и упражнения по разделам представлены на сайте кафедры (Режим доступа: http://cathedra.icc.dgu.m/?id=1479) и образовательном блоге (Режим доступа: https:// baysaidova.blogspot.com/)
3.Электронная версия методических указаний по организации самостоятельной работы представлена на сайте кафедры. Режим доступа: http://cathedra.icc.dgu.ru/?id=1479 4.Электронная библиотека учебных и контрольно-обучающих программ представлена на сайте кафедры. Режим доступа: http://cathedra.icc.dgu.ru/?id=1479 5.Электронная версия тестовых заданий по всем разделам курса имеется в учебнометодическом кабинете кафедры.

Вопросы для самостоятельной работы:

В чем суть содержания и основных составляющих компьютерной безопасности?
Каковы отличительные черты информационного общества?
Каковы основные этапы развития средств информационных коммуникации?
4.Что означают понятия «информация», «информационная безопасность», «информационная безопасность государства?
Кто является потребителем и обладателем (производителем) информации?
Каковы основные объекты и субъекты компьютерной безопасности?
Какие средства обеспечивают информационную безопасность?
Каковы основные категории модели компьютерной безопасности?
Каковы теоретико-методологические основы компьютерной безопасности?
Какие нормативно-правовые акты применяются в области защиты информации?
11.Что собой представляют сопутствующие нормативно-правовые акты по безопасности информации?
Какова структура органов, обеспечивающих информационную безопасность?
Каковы основные направления защиты информационной системы?
Каковы основные составляющие национальных интересов РФ в информационной сфере?
В чем суть внутренних источников угроз компьютерной безопасности РФ?
В чем суть внешних источников угроз компьютерной безопасности РФ?
Каковы общие методы обеспечения компьютерной безопасности РФ?
В чем суть правовых методов обеспечения компьютерной безопасности РФ?
Каковы организационно-технические методы обеспечения компьютерной безопасности РФ?
В чем суть экономических мер обеспечения компьютерной безопасности РФ?
Каковы общие и частные методы обеспечения компьютерной безопасности в различных сферах общественной жизни?
Каковы принципы государственной политики обеспечения компьютерной безопасности РФ?
Каковы направления деятельности государства в процессе реализации его функций по обеспечению компьютерной безопасности РФ?
В чем суть научной проблемы обеспечения компьютерной безопасности РФ?
Каковы пути решения гуманитарных, научно-технических проблем и проблем кадрового обеспечения компьютерной безопасности РФ?

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

Фонд оценочных средств дисциплины включает в себя контрольные вопросы, задания контрольных работ, вопросы для промежуточной аттестации.

Виды самостоятельной работы обучающихся

Изучение основной и дополнительной литературы по материалам курса.

Выполнение заданий самостоятельной работы по курсу.

Таблица 1.1 Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Се местр	Лекции	Лабора торные занятия	Практи ческие занятия	Само-стоя-тельная работа	Автома-тизиро-ванное тести рование	Другие виды учебной дея тельно-	Проме-жуто-чная аттеста ция	Итого
3	5	0	15	35	0	5	40	100

Программа оценивания учебной деятельности студента Семестр 7

Лекции. Посещаемость, опрос, активность за семестр — от 0 до 5 баллов. **Лабораторные занятия. Выполнение одной лабораторной работы – 10б.**

Практические занятия. Посещаемость, опрос, активность за семестр — от 0 до 15 баллов.

Самостоятельная работа.
Контроль выполнения заданий самостоятельной работы в течение одного семестра — от 0 до 25 баллов;
Контрольная работа (от 0 до 10 баллов);
Таким образом, студент в течении 3-го семестра может получить от 0 до 35 баллов.
Автоматизированное тестирование. Не предусмотрено.

Другие виды учебной деятельности.

Написание реферата является одной из форм обучения студентов. Данная форма обучения направлена на организацию и повышение уровня самостоятельной работы студентов. Реферат, как форма обучения студентов - это краткий обзор максимального количества доступных публикаций по заданной теме, подготовка самого реферативного обзора и презентации по нему. При проведении обзора должна проводиться и исследовательская работа, но объем ее ограничен, так как анализируется уже сделанные выводы и в связи с небольшим объемом данной формы работы. Преподавателю предоставляется сам реферат в письменной форме (электронная версия в формате Microsoft Word) и презентация к нему (электронная версия в формате PowerPoint). Сдача реферата происходит в форме защиты доклада с использованием подготовленной презентации.

Критерии оценки контрольной работы:

Оценки на "отлично":

10 - тема раскрыта блестяще, презентация является целостным новым независимым дополнением высокого уровня к лекционному курсу
9 - тема раскрыта отлично, есть отдельные фрагменты, которые являются новыми независимыми смысловыми дополнениями к лекциям
8 - тема в основном раскрыта, качество материала высокое, но не является уникальным

Оценки на "хорошо"

7 - тема раскрыта не полностью, не хватает некоторой части. Качество материала хорошее.
6 - тема раскрыта не полностью, не хватает некоторой значимой части.

Удовлетворительно:

5 - раскрыта хотя бы примерно половина темы. Качество материала удовлетворительное.
4 - что-то по существу реферата сказано, но мало и фрагментарно. Качество материала на грани удовлетворительного.

Неудовлетворительно:

3 - понял, о чем надо рассказывать, но практически ничего не рассказал по теме реферата. Качество материала неудовлетворительное.
2 - понял название темы, ничего не рассказал либо рассказывал не о том. Материал фактически отсутствует.
1 - не понял название темы, не рассказывал. Материал фактически отсутствует и не по теме.
0 - реферат не сдавался.

Промежуточная аттестация. Методика оценивания знаний обучающихся по дисциплине «Технологии обеспечения информационно безопасности» в ходе промежуточной аттестации:
25-40 баллов:
Ответ студента содержит:
глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
знание концептуально-понятийного аппарата всего курса;
знание монографической литературы по курсу,
также свидетельствует о способности:
самостоятельно критически оценивать основные положения курса;
увязывать теорию с практикой.
15-24 баллов:
Ответ студента свидетельствует:
о полном знании материала по программе;
о знании рекомендованной литературы,

а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.
1-14 баллов:
Ответ студента содержит:
поверхностные знания важнейших разделов программы и содержания лекционного курса;
затруднения с использованием научно-понятийного аппарата и терминологии курса;
стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.
Студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала ставится оценка 0 баллов.
Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за один семестр по дисциплине «Технологии обеспечения информационно безопасности» составляет 100 баллов.

Итоговой формой контроля знаний, умений и навыков по дисциплине является **Экзамен**. Экзамен проводится в форме тестирования. При соответствии ответа учащегося на зачете более чем 51 % критериев из этого списка выставляется оценка «удовлетворительно», 66% – 85% оценка «хорошо», 86% и выше оценка «отлично».

8. Учебно-методическое и информационное обеспечение дисциплины

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

А) Основная литература:

1.Галатенко В.А. Основы компьютерной безопасности. - М., 2007 http://www.wciom.ru/
2.Колин К.К. Гуманитарные аспекты компьютерной безопасности. - М., 2008 http://www.romir.ru/ 3.Минаев В.А., Фисун А.П. Правовое обеспечение компьютерной безопасности. - М., 2008 http://www.romir.ru/
4.Основы компьютерной безопасности. Учебное пособие. / Под ред. О.А.Акулова, Д.Н.Баданина. - М.,2008
4.Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение компьютерной безопасности. - М., 2008 www.wikipedia.org

В) Дополнительная литература:

1.ГОСТ РИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента компьютерной безопасности. Требования. www.academic.ru
2.Галатенко В.А. Стандарты компьютерной безопасности. - М., 2008
Петренко С.А., Курбатов В.А. Политика компьютерной безопасности. - М., 2007 http://www.wciom.ru/
4.Тихонов В., Райх В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. - М., 2006
Ярочкин В.И. Информационная безопасность. - М.,2007 http://www.romir.ru/

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

ВЦИОМ - http://www.wciom.ru/
Гуманитарные науки - http://www.humanus.site3k.net Портал «Гуманитарное образование» - www.humanities.edu.ru Портал словарей - www.slovari.yandex.ru
Российский независимый институт социальных и национальных проблем - http://www.riisnp.m/
Социологические исследования - www.ecsocman.edu.ru Учебный портал - www.academic.ru
Федеральный портал «Российское образование» - www.edu.ru Электронная библиотека - www.gumer.info

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1.Прохоренок, Н. А. Python. Самое необходимое — Санкт-Петербург : БХВ- Петербург, 2010.

http://znanium.com/go.php?id=354989 (Электронный ресурс)
2.Максимов, К В. Компьютерные сети —Москва : Издательство «ФОРУМ», 2008. http://znanium.com/go.php?id=l63728 (Электронный ресурс)
Понимаете ли вы что такое облачные вычисления (cloud computing) http://habrahabr.ru/post/74740/
Демонстрация работы с OpenStack версии Grizzly (через Horizon) http://www. youtube. com/watch?v=p4eW78gHfCg
3. Официальный сайт OpenStack http://www.openstack.org/
Перевод книги OpenStack Beginner's Guide for Ubuntu — Natty
http://xgu.ru/wiki/nepeBOA_KHnru_OpenStack_Beginner's_Guide_for_Ubuntu_-_Natty

10. Материально-техническое обеспечение учебной дисциплины «Технологии обеспечения информационно безопасности»
Лекционная аудитория с мультимедийным оборудованием и с выходом в Интернет.
Компьютерный класс с оборудованием для показа мультимедийных презентаций, с возможностью работы под управлением операционной системы Linux, с подключением к Интернет, рассчитанный на обучение группы студентов из 8-12 человек, удовлетворяющий санитарно-гигиеническим требованиям.

11.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе: – ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы); – мультимедийный проектор с дистанционным управлением. Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены персональными компьютерами с возможностью подключения к сети Интернет

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

При освоении дисциплины для выполнения лабораторных работ необходимы классы персональных компьютеров с приложениями программирования на языках C/C++. Для проведения лекционных занятий, необходима мультимедийная аудитория с набором лицензионного базового программного обеспечения.

Лекционные занятия

- Видеопроектор, ноутбук, презентатор
- Подключение к сети Интернет

Практические занятия

- Видеопроектор, ноутбук
- Подключение к сети Интернет