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

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД.03 Информационная безопасность
(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки: 27.03.03 Системный анализ и управление
(код и наименование направления подготовки/специальности)

Направленность (профиль):
Интеллектуальная бизнес-аналитика и управление экономическими процессами
(наименование направленности (профиля) / специализации)

Форма обучения: очная
(очная, очно-заочная, заочная)

Квалификация: бакалавр

Краснодар 2024

Рабочая программа дисциплины **Информационная безопасность**
составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 27.03.03 Системный анализ и управление

Программу составил(и):

Коваленко А.В., доцент, канд. экон. наук, доцент 

Рабочая программа дисциплины **Информационная безопасность**
утверждена на заседании кафедры экономики предприятия, регионального и кадрового менеджмента
протокол № 6 « 29 » февраля 2024г.

Заведующий кафедрой  Вукович Г.Г

Утверждена на заседании учебно-методической комиссии факультета
протокол № 9 «14»мая 2024г.
Председатель УМК факультета  Дробышевская Л.Н.

Рецензенты:

Прокуратов Д.П., директор ООО «Бизнес процессы», кандидат экономических наук

Кизим А.А.,доктор экономических наук, профессор кафедры мировой экономики и менеджмента Кубанского государственного университета

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Формирование знаний основных составляющих информационной безопасности государства, общества, предприятия (организации) и личности; умений и навыков использования организационных, правовых, инженерно-технических и аппаратно-программных методов и средств при построении систем информационной безопасности в области выбранного профиля подготовки.

1.2 Задачи дисциплины

Знакомство с современными и классическими концепциями информационной безопасности; углубление знаний в области научных представлений об информационной безопасности; развитие навыков информационной безопасности, сформировать у студентов необходимый объем знаний и навыков по дисциплине «**Информационная безопасность** в области способности работать в коллективе не допуская клевету и распространение сведений, порочащих иные организации и коллег, соблюдая конфиденциальность информации и не разглашать материалы рабочих исследований, ориентироваться в процессах всесторонней защиты информации при решении профессиональных задач

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «**Информационная безопасность**» относится к части, формируемой участниками образовательных отношений ФТД «Факультативные дисциплины» учебного плана. В соответствии с рабочим учебным планом дисциплина изучается на 2 курсе по очной форме обучения. Вид промежуточной аттестации: зачет.

Изучение дисциплины базируется на курсе Информационно-коммуникационные технологии в профессиональной деятельности, Профессиональные компьютерные программы. Представленная дисциплина является основой дальнейшего изучения таких дисциплин как Компьютерные системы и сети, Организационно-управленческая практика, Подготовка к процедуре защиты выпускной квалификационной работы, Защита выпускной квалификационной работы и ряда других.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
ИУК-1.1 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Знает: принципы защиты информации на предприятии
	Умеет: не допускать клевету и распространение сведений, порочащих иные организации и коллег, соблюдать конфиденциальность информации и не разглашать материалы рабочих исследований
	Трудовое действие: организует расчетно-аналитическую деятельность с учетом требований конфиденциальности.
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
ИУК-1.2 Выбирает оптимальный вариант решения задачи, аргументируя свой выбор	Знает: современные и классические концепции информационной безопасности.
	Умеет: определять и предотвращать угрозы информации при решении профессиональных задач
	Трудовое действие: использует современные средства

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	защиты информации
ОПК-7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ИОПК-7.1 Применяет базовые компьютерные и программные средства для решения профессиональных задач	Знает: принципы соблюдения цифровой гигиены
	Умеет: определять и предотвращать угрозы информации при решении профессиональных задач
	Трудовое действие: использует современные средства профилактики цифрового здоровья

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зачетных единицы (72 часа), их распределение по видам работ представлено в таблице

Виды работ		Всего часов	Форма обучения			
			очная		очно-заочная	заочная
			3 семестр (часы)	X семестр (часы)	X семестр (часы)	курс (часы)
Контактная работа, в том числе:						
Аудиторные занятия (всего):			**34**	-	-	
занятия лекционного типа			18	-	-	
лабораторные занятия			-	-	-	
практические занятия			16	-	-	
семинарские занятия			-	-	-	
Иная контактная работа:				-	-	
Контроль самостоятельной работы (КСР)			2	-	-	
Промежуточная аттестация (ИКР)			0,2	-	-	
Самостоятельная работа, в том числе:			**35,8**	-	-	
Подготовка к деловой игре «Информационная защита предприятия (организации)»			10	-	-	
Реферат (доклад-презентация) (подготовка)			10	-	-	
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным занятиям, тестированию по разделам дисциплины.)			15,8	-	-	
Контроль:				-		
Подготовка к экзамену			-	-	-	
Общая трудоемкость	**час.**		**72**		-	
	в том числе контактная работа		**36,2**		-	
	зач. ед		**2**		-	

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 3 семестре (2 *курсе*)***(очная** форма обучения)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Раздел 1. Введение в дисциплину	14	4	4	-	6
2.	Раздел 2. Основы государственной политики РФ в области информационной безопасности	18	4	4	-	10
3.	Раздел 3. Информационная война.	18,8	4	4	-	9,8
4.	Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС)	20	6	4	-	10
	ИТОГО по разделам дисциплины	67,8	18	16	-	35,8
	Контроль самостоятельной работы (КСР)	2	-	-	-	-
	Промежуточная аттестация (ИКР)	0,2	-	-	-	-
	Подготовка к текущему контролю		-	-	-	-
	Общая трудоемкость по дисциплине	72	-	-	-	

Примечание: Л – лекции, ПЗ – практические занятия / семинары,ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1.	Раздел 1. Введение в дисциплину	Раздел 1. Введение в дисциплину 1.1 Понятие национальной безопасности РФ 1.2 Виды безопасности 1.3 Информационная безопасность в системе национальной безопасности РФ 1.4 Роль информационной безопасности в обеспечении национальной безопасности государства	Л,Д
2.	Раздел 2. Основы государственной политики РФ в области информационной безопасности	Раздел 2. Основы государственной политики РФ в области информационной безопасности 2.1 Национальные интересы РФ в информационной сфере и их обеспечение 2.2 Виды угроз информационной безопасности РФ 2.3 Источники угроз информационной безопасности 2.4 Основные направления обеспечения информационной безопасности государства	Л,Д
3.	Раздел 3. Информационная война.	Раздел 3. Информационная война. 3.1 Методы и средства ее ведения 3.2 Информационная безопасность и информационное противоборство 3.3 Информационное оружие, его	Л,Д

		классификация и возможности 3.4 Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны	
4.	Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС)	Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС) 4.1 Организационно-правовые основы информационной безопасности КС 4.2 Организационно-технические основы ИБ КС 4.3 Аппаратно-программные средства обеспечения ИБ КС 4.4 Основы комплексного обеспечения ИБ КС	Л,Д

2.3.2 Занятия семинарского типа (практические / семинарскиезанятия/лабораторные работы)

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
1.	Раздел 1. Введение в дисциплину	Изучение методов защиты от разрушающих программных воздействий при помощи программных комплексов антивирусной защиты	ЛР
2.	Раздел 2. Основы государственной политики РФ в области информационной безопасности	Изучение методов защиты при помощи программно-аппаратного комплекса Secret Net	ЛР
3.	Раздел 3. Информационная война.	" Шифрование и обмен шифрованной информацией с использованием системы «PGP»	ЛР,Р
4.	Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС)	Применение специализированных средств организации VPN на примере «OpenVpn»	ЛР, ДИ

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), реферата(доклада)-презентации (РП), эссе (Э), коллоквиум (К), тестирование (Т), опрос (О), лекция (Л), составление тезисов по первоисточнику (Т), дискуссия (Д), разработка индивидуальных заданий (проектов) (ИЗ), подготовка к деловой игре (ДИ) и т.д.

2.3.3 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены учебным планом.

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	Занятия лекционного и семинарского типа	Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года.. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
2	Подготовка эссе, рефератов, курсовых работ.	Методические указания для подготовки эссе, рефератов, курсовых работ. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года.. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
3	Выполнение самостоятельной работы обучающихся	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года.. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
4	Выполнение расчетно-графических заданий	Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года.. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
5	Интерактивные методы обучения	Методические указания по интерактивным методам обучения. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya

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,

– в форме аудиофайла,

– в печатной форме на языке Брайля.

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,

– в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии, применяемые при освоении дисциплины (модуля)

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, практические занятия, проблемное обучение, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов(проектных методик, мозгового штурма, разбора конкретных ситуаций, иных форм) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

5. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «**Информационная безопасность предприятия (организации)».**

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме доклада-презентации по проблемным вопросам, заданий, и **промежуточной аттестации** в форме вопросов и заданий к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименованиеоценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИУК-1.1 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Знает: принципы защиты информации на предприятии	Вопросы для устного опроса по теме. Темы для дискуссий на лекционных занятиях. Реферат (доклад-презентация)	Вопрос на зачете 1-8
2	ИУК-1.1 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Умеет: не допускать клевету и распространение сведений, порочащих иные организации и коллег, соблюдать конфиденциальность информации и не разглашать материалы рабочих исследований	Вопросы для устного опроса по теме. Темы для дискуссий на лекционных занятиях. Выполнение заданий для подготовки к деловой игре.	Вопрос на зачете 1-8
3	ИУК-1.1 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Трудовое действие: организует расчетно-аналитическую деятельность с учетом требований конфиденциальности.	Вопросы для устного опроса по теме. Темы для дискуссий на лекционных занятиях. Выполнение заданий для подготовки к деловой игре.	Вопрос на зачете 1-8
4	ИУК-1.2 Выбирает оптимальный вариант решения задачи, аргументируя свой выбор	Знает: современные и классические концепции информационной безопасности. Умеет: определять и предотвращать угрозы информации при решении профессиональных задач Трудовое действие: использует современные средства защиты информации	Вопросы для устного опроса по теме. Темы для дискуссий на лекционных занятиях. Выполнение заданий для подготовки к деловой игре.	Вопрос на зачете 9-15
5	ИОПК-7.1 Применяет базовые компьютерные и программные средства для решения профессиональных задач	Знает: принципы соблюдения цифровой гигиены Умеет: определять и предотвращать угрозы информации при решении профессиональных задач	Вопросы для устного опроса по теме. Темы для дискуссий на лекционных занятиях. Выполнение заданий для подготовки к деловой игре.	Вопрос на зачете 16-24
6	ИОПК-7.1 Применяет базовые компьютерные и программные средства	Трудовое действие: использует современные средства профилактики	Вопросы для устного опроса по теме. Темы для дискуссий на лекционных	Вопрос на зачете 25-36

	для решения профессиональных задач	цифрового здоровья	занятиях. Выполнение заданий для подготовки к деловой игре.	

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

Примерный перечень вопросов и заданий

Вопросы для устного опроса по разделу

Раздел 1. Введение в дисциплину

1.1 Понятие национальной безопасности РФ

1.2 Виды безопасности

1.3 Информационная безопасность в системе национальной безопасности РФ

1.4 Роль информационной безопасности в обеспечении национальной безопасности государства

Раздел 2. Основы государственной политики РФ в области информационной безопасности

2.1 Национальные интересы РФ в информационной сфере и их обеспечение

2.2 Виды угроз информационной безопасности РФ

2.3 Источники угроз информационной безопасности

2.4 Основные направления обеспечения информационной безопасности государства

Раздел 3. Информационная война.

3.1 Методы и средства ее ведения

3.2 Информационная безопасность и информационное противоборство

3.3 Информационное оружие, его классификация и возможности

3.4 Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны

Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС)

4.1 Организационно-правовые основы информационной безопасности КС

4.2 Организационно-технические основы ИБ КС

4.3 Аппаратно-программные средства обеспечения ИБ КС

4.4 Основы комплексного обеспечения ИБ КС

Темы для дискуссии на лекционных занятиях
по разделам дисциплины

Основные определения и положения теории информационной безопасности

Основные положения доктрины информационной безопасности РФ

Место информационной безопасности в системе национальной безопасности

Обобщенная модель системы защиты от угроз нарушения конфиденциальности информации

Определение экономической безопасности организации.

Уровень экономической безопасности как основная характеристика экономической безопасности организации.

Источники угроз экономической безопасности организации.

Основные типы и характеристики негативных воздействий на экономическую безопасность организации.

Цели экономической безопасности организации.

Способы обеспечения экономической безопасности организации.

Критерии и показатели экономической безопасности организации.

Методы оценки экономической безопасности организации.

Основные направления обеспечения экономической безопасности организации.

Функциональные составляющие экономической безопасности организации.

Критерии оценки и способы обеспечения финансово-экономической безопасности организации.

Критерии оценки и способы обеспечения технологической безопасности организации.

Экологическая безопасность организации.

Критерии оценки и способы обеспечения информационной безопасности организации.

Основные определения формальной теории защиты информации

Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».

Информационная безопасность человека и общества и государства.

Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.

Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.

Правовые средства защиты информации. Защита программных продуктов. Авторское право.

Структуризация методов обеспечения информационной безопасности.

Основные методы реализации угроз информационной безопасности.

Основные принципы обеспечения информационной безопасности в автоматизированной системе.

Причины, виды и каналы утечки информации.

Методы построения защищенных автоматизированных систем.

Политика безопасности. Основные типы политики безопасности.

Политика безопасности. Модели безопасности.

Монитор безопасности обращений

Формальные модели управления доступом

Ролевое управление доступом

Скрытые каналы передачи информации

Основы методологии защиты информации

Классификация методов ЗИ

Организационные меры и меры обеспечения физической безопасности

Методы идентификации и аутентификации

Методы разграничения доступа

Криптографические методы обеспечения целостности информации

Построение систем защиты от угроз нарушения доступности

История криптографии, основные понятия и определения, требования к криптографическим системам.

Задания для практических занятий

Занятие 1 Изучение методов защиты от разрушающих программных воздействий при помощи программных комплексов антивирусной защиты

Произвести настройки постоянной защиты, пояснить действия.

Все антивирусные программы имеют в своем составе резидентную часть, которая запускается при загрузке компьютера, постоянно находится в оперативной памяти и в

режиме реального времени отслеживает "подозрительные события", в частности, попытки запуска инфицированных программ.

Произвести настройки проверки всех файлов, пояснить действия.

Этот режим для повышение уровня защищенности. Он замедляет процесс сканирования, но обеспечивает более надежную защиту. Часто вирусы находятся в заархивированных файлах (.zip, .arj...); нередко вредоносные программы распространяются в файлах с измененными расширениями (.txt, .jpg и т.п.).

Произвести настройки режима эвристического анализа, пояснить действия.

Позволяет по ряду косвенных признаков выявлять файлы, возможно содержащие новые, неизвестные вирусы, а также отслеживать "подозрительные события" на вашем компьютере. Большинство антивирусных программ имеет несколько уровней эвристического анализа (чаще всего три) и возможность его вообще отключить. Рекомендуется установить средний уровень. Максимальный уровень эвристического сканирования, конечно, повышает степень защиты, но сильно замедляет работу и дает большое количество ложных срабатываний. Его имеет смысл включать, если есть информация о предстоящей или уже начавшейся атаки нового, ранее неизвестного вируса.

Произвести настройки действия антивирусной программы при обнаружении вируса. Пояснить действия.

Обычно имеется возможность установить один из следующих режимов:

только отчет;

лечить зараженные файлы; если вылечить невозможно:

- удалять зараженные файлы;
- переименовывать, перемещать зараженные файлы;
- запрашивать пользователя о дальнейших действиях

сразу удалять зараженные файлы.

Рекомендуется установить режим "лечить зараженные файлы; если вылечить невозможно, запрашивать пользователя о дальнейших действиях".

Произвести настройки автоматического обновления программы и антивирусных баз. Пояснить действия.

Эта опция позволяет автоматически скачивать через интернет с сайта разработчика все последние изменения. Рекомендуется включить и установить в расписании "ежедневно" в удобное для пользователя время, например ночью.

Произвести настройки автоматического сканирования. Пояснить действия.

Если компьютер включен постоянно, то рекомендуется запускать ежедневно в удобное время, например ночью, сразу после обновления программы и антивирусных баз.

Занятие 2 Изучение методов защиты при помощи программно-аппаратного комплекса Secret Net

Произвести настройки следующих параметров, пояснить действия.

Полномочное (мандатное) и дискреционное разграничение доступа.

Усиленная аутентификация пользователей, в том числе с поддержкой идентификаторов и сертификатов.

Контроль целостности и создание доверенной информационной среды.

Контроль утечек и каналов распространения информации.

Защита терминальной и VDI-инфраструктуры.

Централизованное управление, мониторинг и аудит.

Поддержка иерархии и резервирования серверов безопасности в распределенных инфраструктурах.

Построение отчетов о состоянии системы.

Интеграция со средством доверенной загрузки ПАК «Соболь».

Обеспечение процесса расследования инцидентов с помощью подробных журналов, отчетов и системы теневого копирования отчуждаемой информации.

Демо версия Secret Net (Российский разработчик программных и аппаратных средств защиты информации. «Код Безопасности») для выполнения используется с электронного ресурса открытого доступа: https://www.securitycode.ru/products/demo-versions/

Занятие 3" Шифрование и обмен шифрованной информацией с использованием системы «PGP»

Принципы работы PGP шифрования

OpenPGP-совместимое средство для шифрования и цифровой подписи сообщений в Thunderbird и Seamonkey.

PGP шифрование в Mozilla Thunderbird с дополнением Enigmail.

Настроить PGP шифрование в Mozilla Thunderbird с дополнением Enigmail. Переслать письмо в PGP шифрование в Mozilla Thunderbird с дополнением Enigmail.

Ключи для секретных замков, цифровая подпись, ключевая пара, ограничения использования PGP. Области применения PGP.

PGP Desktop 9.5 beta демо версия.

Произвести настройки системы, передать сообщение.

Занятие 4 Применение специализированных средств организации VPN на примере «OpenVpn» Способы защиты программ от дизассемблирования

Произвести настройки OpenVPN

Настройки анонимности.

Построение туннелей и соединение через прокси сервер.

Подключение VPN клиента.

Демо версия OpenVPN для выполнения задания используется с электронного ресурса открытого доступа: http://free-vpn.ru/openvpn.html

Реферат (доклад-презентация)

Тематика рефератов

История развития криптографии.

Классификация криптографических систем.

Законодательные и правовые основы защиты компьютерной информации и информационных технологий

Энтропия, теоретическая и практическая стойкость, вычислительная стойкость. Теоретико-информационная стойкость.

Вычислительная и временная сложность алгоритма.

Шифр DES, режимы работы DES

Шифр AES

Шифр ГОСТ 28147-89.

Поточные шифр РСЛОС

Шифр RC4

Шифр Рона

Выбор ключа, время жизни ключа, разделение секрета.

Схема обмена секретными ключами: широкоротой лягушки

Схема обмена секретными ключами - Ниджейма-Шредера
Протоколы основанные на эллиптических кривых
Общая схема функционирования систем с открытыми ключами.
Криптосистема RSA и ее модификации.
Криптосистема Эль Гамаля.
Криптосистема Рабина
Алгоритмы ЭЦП: Нибберга-Руппеля
Характеристика протоколов идентификации и аутентификации
Идентификация на основе пароля.
Взаимная проверка подлинности пользователей.
Идентификация с нулевой передачей знаний.
Схемы обязательств.
Системы электронного голосования.
Системы перераспределения доверия: PGP
Системы перераспределения доверия: SSL
Системы перераспределения доверия: X509 (PKIX)
Системы перераспределения доверия: SPKI
Неявные сертификаты
Виды атак: Атака Винера на RSA
Атаки на RSA основанные на решетках
Атака Хостада
Атака Франклина-Рейтера
Частичное раскрытие ключа
Стойкость актуальных алгоритмов шифрования

Задание для деловой игры

На практических занятиях группа делится на две примерно равные по количеству и потенциалу подгруппы.

Каждая из подгрупп представляет собой конкурирующую организацию (предприятие). Название, профиль деятельности (одинаковый для обоих предприятий) обычно предлагают студенты.

Задачей каждого «отдела» является – разработка максимального количества потенциальных угроз утраты, порчи, искажения соответствующей информации и мер противодействия этим угрозам- с одной стороны, и максимального количества способов получения, порчи, искажения информации отдела-конкурента-с другой.

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен/<u>зачет</u>)

Вопросы к зачету

1. Информационная безопасность человека и общества и государства.
2. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
3. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
4. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
5. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.
6. Методы и средства защиты информации.
7. Содержание способов и средств обеспечения безопасности информации.
8. Реализация методов и средств защиты информации.
9. Средства опознания и разграничения доступа к информации.

10. Криптография. Симметричные криптосистемы.
11. Криптография. Асимметричные криптосистемы.
12. Обзор и классификация методов шифрования информации.
13. Электронно-цифровая подпись.
14. Основные алгоритмы шифрования данных: ГОСТ.
15. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
16. Защита данных в автономном компьютере.
17. Защита данных в вычислительных сетях.
18. Разработка сетевых аспектов политики безопасности.
19. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
20. Показатели оценки достоверности (безошибочности) передачи данных в сетях.
21. Методы взлома компьютерных систем: атаки на уровне операционных систем, атаки на уровне программного обеспечения, атаки на уровне систем управления базами данных.
22. Парольная защита операционных систем.
23. Парольные взломщики.
24. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
25. Структуризация методов обеспечения информационной безопасности.
26. Основные методы реализации угроз информационной безопасности.
27. Основные принципы обеспечения информационной безопасности в автоматизированной системе.
28. Причины, виды и каналы утечки информации.
29. Методы построения защищенных автоматизированных систем.
30. Политика безопасности. Основные типы политики безопасности.
31. Политика безопасности. Модели безопасности.
32. Стандарты информационной безопасности.
33. Правовое обеспечение защиты информации. Нормативные документы.
34. Разрушающие программные воздействия: вирусы и закладки.
35. Антивирусные средства.
36. Психологические аспекты информационной безопасности организации.

Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает современные и классические концепции информационной безопасности, современные инструменты и методы защиты информации, допускает незначительные ошибки; студент умеет правильно определять угрозы информации, иллюстрируя примерами формулировок и ситуаций возникновения угроз конфиденциальности информации.

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры по ряду элементов понятийного аппарата дисциплины, довольно ограниченный объем знаний программного материала.

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.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Учебная литература

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 216 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820. - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1784437

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326

Дополнительная литература

5.2. Периодическая литература

1. Базы данных компании «Ист Вью»http://dlib.eastview.com
2. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ»https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wileyhttps://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ)http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОНhttp://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцинаhttps://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка(http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование"http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам"http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсовhttp://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском"https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык"http://gramota.ru/;
11. Служба тематических толковых словарейhttp://www.glossary.ru/;
12. Словари и энциклопедииhttp://dic.academic.ru/;
13. Образовательный портал "Учеба"http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответыhttp://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обученияhttp://moodle.kubsu.ru

2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологийhttp://mschool.kubsu.ru;
4. Электронный архив документов КубГУhttp://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

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

– Общие рекомендации по самостоятельной работе обучающихся;

Самостоятельная работа предусматривает самостоятельное освоение отдельных вопросов и проблем в рамках учебной дисциплины. В процессе самостоятельной работы слушатели знакомятся с содержанием научных статей и монографий, составляют тезисы, осуществляют подготовку к семинарским занятиям, опираясь на список литературы и дополнительные списки к темам самостоятельной подготовки.

– Методические рекомендации по освоению лекционного материала, подготовке к лекциям;

Лекция является главной, важнейшей формой учебных занятий по дисциплине. На лекции излагаются основы теоретических знаний, создаются условия и осуществляются воспитательные цели по формированию специалиста, способного находить и практически осмысливать пути решения теоретических и практических задач. На лекциях излагаются основные положения науки, их доказательства, методические приемы, история ее развития, применимость в других научных дисциплинах.

Лекционный курс в полной мере определяет содержание практических занятий, расчетно-графических работ и других видов самостоятельной работы студентов по дисциплине.

Главным показателем качества лекции является ее научный уровень. Лекция должна содержать фундаментальные положения, узловые вопросы, доказательства приводимых положений, глубоко раскрывать неразрывную связь дисциплины с Кейс-стадии, возникающими в ходе практической деятельности.

Научный уровень лекции зависит от квалификации преподавателя, его непрерывного совершенствования, научного роста. Акцентирование внимания на том или другом положении будет правильным при высокой общетеоретической подготовке преподавателя, его способности понимать научно-технические задачи, возникающие на современном этапе.

В структуре учебного процесса на лекции отводится около половины учебного времени. Существенное значение имеет объем учебного материала, выносимого на лекцию. В любом случае должны быть обеспечены глубокое раскрытие существа вопроса и достаточно интенсивная работа студентов.

Основа учебного материала содержится в учебнике. Это не означает, что устное изложение должно повторять содержание учебника. Лектор практически всегда может найти более четкое и экономное изложение доказательств, не снижая его строгости и общности.

Именно лекции, как основной вид занятия, обеспечивают большую воспитательную силу занятия. В связи с этим при подготовке лекции особенно тщательно отрабатываются мировоззренческие вопросы курса.

Лектор обязан пользоваться стандартными терминологией, обозначениями и единицами измерения. Это обстоятельство существенно, так как в имеющейся литературе есть много отклонений от этих требований.

Вступительная часть лекции разделяется на организационную, связанную с проверкой готовности аудитории к началу лекции, и постановку задачи на занятие.

Постановка задачи на занятие дается в произвольной форме, и как правило, содержит в себе:

- краткое напоминание о предшествующих занятиях, на которых рассматривались отправные данные для данной лекции вопросы, излагалось решение аналогичной задачи в другой постановке или при других предпосылках и т.п.;
- объяснение цели занятия.

Это очень важный момент лекции. Студентам должна быть ясна необходимость исследования новой задачи или проблемы. Здесь часто целесообразно обращаться к истории возникновения изучаемой задачи, показ важности ее для практических целей. При постановке задачи важно заинтересовать студентов предстоящим занятием.

При постановке задачи должна быть названа изучаемая тема, сообщено название занятия и учебные вопросы, подлежащие отработке. Часто целесообразно предварительно ориентировать на степень сложности и важности вводимых понятий или математических выкладок.

– Методические рекомендации по подготовке к семинарским (практическим/лабораторным) занятиям.

Содержание семинарских занятий определяется календарным тематическим планом, который составляется на основе рабочей программы дисциплины и утверждается заведующим кафедрой.

В начале каждого занятия преподаватель проводит краткое обсуждение трудностей, возникших в ходе выполнения заданий, полученных на предыдущем занятии, после чего напоминает студентам основные понятия, формулы и методы по той теме, которая изучается на данном занятии.

Затем начинается решение практических задач (примеров) по теме занятий. Первую задачу по каждому разделу темы решает преподаватель.

Далее преподаватель либо записывает тексты нескольких задач на доске, либо записывает номера этих задач по задачнику, имеющемуся у студентов, и предлагает студентам самостоятельно решить эти задачи, при необходимости, используя компьютеры.

Некоторое время преподаватель наблюдает, как студенты решают и, если дела идут успешно, приглашает одного из студентов к доске для решения очередной задачи.

Если же у студентов возникают трудности, преподаватель сам приступает к решению задачи на доске, но делает это медленно с подробным разбором каждого шага решения и с обязательным вовлечением студентов группы в процесс обсуждения алгоритма решения задачи. И так далее, переходя от задачи к задаче, пока не завершится занятие.

В конце занятия преподаватель задает студентам задание по самостоятельному решению нескольких задач дома (для закрепления навыков решения) или варианты индивидуальных расчетных заданий.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

Практическое занятие предполагает свободный обмен мнениями по избранной тематике. Он начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, заслушиваются сообщения студентов, решаются задачи, тесты. Обсуждение сообщения

совмещается с рассмотрением намеченных вопросов и решением задач. Сообщения, предполагающие анализ публикаций по отдельным вопросам, заслушиваются обычно в середине занятия. Поощряется выдвижение и обсуждение альтернативных мнений. В заключительном слове преподаватель подводит итоги обсуждения и объявляет оценки выступавшим студентам. В целях контроля подготовленности студентов и привития им навыков краткого письменного изложения своих мыслей преподаватель в ходе практических занятий может осуществлять текущий контроль знаний в виде тестовых заданий.

При подготовке к практическому занятию студенты имеют возможность воспользоваться консультациями преподавателя. Кроме указанных тем студенты вправе, по согласованию с преподавателем, избирать и другие интересующие их темы.

Качество учебной работы студентов преподаватель оценивает в конце занятия, выставляя в рабочий журнал текущие оценки. Студент имеет право ознакомиться с ними.

Одна из эффективных форм освоения учебного материала – это подготовка сообщений, рефератов. Сообщение – это самостоятельная работа, анализирующая и обобщающая публикации по заданной тематике, предполагающая выработку и обоснование собственной позиции автора в отношении рассматриваемых вопросов. Подготовка сообщения – достаточно кропотливый труд. Его написанию предшествует изучение широкого круга философских первоисточников, монографий, статей, обобщение личных наблюдений. Работа над сообщением способствует развитию самостоятельного, творческого мышления, учит применять экономические знания на практике при анализе актуальных социальных и правовых проблем. Рекомендуемое время сообщения - 10-12 минут.

– Методические рекомендации по подготовке к деловой игре

Выполнение заданий по подготовке к деловой игре направлено на углубление теоретических знаний, формирование практических умений и навыков работать в коллективе соблюдая конфиденциальность,, необходимой для решения профессиональных задач

На практических занятиях группа делится на две примерно равные по количеству и потенциалу подгруппы.

Каждая из подгрупп представляет собой конкурирующую организацию (предприятие). Название, профиль деятельности (одинаковый для обоих предприятий) обычно предлагают студенты.

Детализируется набор бизнес процессов предприятия и его орг. структуры (выделяют отделы, цеха и др.). Предложенный набор также одинаков для обоих предприятий. Например, служба сбыта, маркетинговый отдел, основное производство (можно по цехам), служба безопасности, ИТ-отдел и т.д.

Студенты делятся в каждой подгруппе на «сотрудников» соответствующих подразделений (обычно не более 2 человек). Например, маркетинговый отдел ООО «Х» : Петров А.С., Чистякова В.А., маркетинговый отдел ООО «У»: Свиблова С.И., Шуйская В.А. и т.д.

Задачей каждого «отдела» является – разработка максимального количества потенциальных угроз утраты, порчи, искажения соответствующей информации и мер противодействия этим угрозам- с одной стороны, и максимального количества способов получения, порчи, искажения информации отдела-конкурента-с другой.

Перед проведением дел.игры каждый «отдел» сдает запечатанный конверт, заклеенный лист бумаги и т.п. преподавателю, где содержится информация о предпринятых мерах по противодействию угрозам утраты, порчи, искажения информации и мерах противодействия возможным угрозам со стороны конкурента.

Представители «отделов» обмениваются «ударами». В начале один отдел пытается получить информацию-другой парирует выпады согласно ранее сданным перечням преподавателю, затем наоборот. Для исключения спорных ситуаций преподаватель

контролирует процесс ориентируясь по вскрытому в присутствии группы конверту, листу и т.п. За каждый успешный элемент (информация получена т.к. действенной защиты не предусмотрено) присуждается 1 балл. Выигрывает команда набравшая большее кол-во баллов.

Примечания.

В процессе формулировки задания и профиля деятельности фирмы называется известный реальный производитель, желательно с некоторыми индикаторами его хозяйственной деятельности. С целью понимания доступности использования методов защиты и получения информации. Соответственно, предлагаемые нереальные по техническим или финансовым соображениям методы должны быть отброшены, хотя и озвучены студентами. А команда может быть оштрафована на 1 балл.

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.

7. Материально-техническоеобеспечение по дисциплине (модулю)

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Учебные аудитории для проведения лабораторных работ Лаборатория информационных и управляющих систем 201Н Лаборатория экономической информатики 202Н	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютеры, ноутбуки Оборудование: ПК, Терминальные станции, Усилитель автономный беспроводной	Microsoft Windows 8, 10, Microsoft Office Professional Plus 1С: Предприятие 8 SPSS Statistics

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения

Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Помещение для самостоятельной работы обучающихся (ауд.213 А, 218 А)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Microsoft Windows 8, 10, Microsoft Office Professional Plus