

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

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования и развитию
проректор

_____ подпись
«25» мая 2022 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Б1.В.16 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
ФИНАНСОВОЙ СФЕРЕ

Направление подготовки / специальность 38.03.01 Экономика
Направленность (профиль) / специализация Финансы и кредит
Форма обучения Очная, очно-заочная
Квалификация Бакалавр

Краснодар 2022

Рабочая программа дисциплины «Основы информационной безопасности в финансовой сфере» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 38.03.01 Экономика

Программу составил (и):

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

Рабочая программа дисциплины «Основы информационной безопасности в финансовой сфере» утверждена на заседании кафедры экономического анализа, статистики и финансов протокол № 7 от 11 мая 2022 г.

Заведующий кафедрой экономического анализа, статистики и финансов

Л.Н. Дробышевская, доктор экон. наук, профессор

Утверждена на заседании учебно-методической комиссии экономического факультета протокол № 11 от 17 мая 2022 г.

Председатель УМК факультета

Л.Н. Дробышевская

доктор экон. наук, профессор

Рецензенты:

Коржевский А.Ю., ген. директор ООО «ЗВСК-Инвест»

Захарова Л.Н., канд. экон. наук, доцент кафедры экономики предприятия, регионального и кадрового менеджмента ФГБОУ ВО «Кубанский государственный университет»

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины – освоение теоретических основ обеспечения информационной безопасности, основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения в организациях финансово-кредитной сферы.

1.2 Задачи дисциплины

– формирование представлений о видах информации, информационной безопасности и организации защиты информации для потребителей финансовых услуг и финансовых организаций;

– формирование знаний об основных способах защиты информации в условиях цифровой экономики;

– формирование умения выбирать и анализировать методы и средства защиты финансовой информации в целях противодействия компьютерной преступности в кредитно-финансовой сфере;

– развитие навыков работы с нормативными правовыми актами и нормативными методическими документами в области обеспечения информационной безопасности банков и других организаций финансовой сферы;

– развитие навыков определения видов угроз информационной безопасности для потребителей финансовых услуг и финансовых организаций.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Основы информационной безопасности в финансовой сфере» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» учебного плана. В соответствии с рабочим учебным планом дисциплина изучается в 6 семестре 3 курса по очной и очно- заочной форме обучения. Вид промежуточной аттестации: зачет.

Дисциплина изучается после ряда гуманитарных, математических, общеэкономических и специальных дисциплин, позволяющих наиболее эффективно усваивать учебный материал в рамках данного курса. Для успешного усвоения дисциплины необходимы базовые знания и навыки в области следующих дисциплин: «Информационно-коммуникационные технологии в профессиональной деятельности», «Профессиональные компьютерные программы», «Нормативно-правовое регулирование финансово-кредитных отношений».

1.4 Перечень планируемых результатов обучения по дисциплине, 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
ПК-1 Способен консультировать клиентов по использованию финансовых продуктов и услуг	
ИПК-1.9 Анализирует базы данных и применяет информационные системы в профессиональной сфере в целях обеспечения информационной безопасности	Знает понятие и виды угроз информационной безопасности в финансовой сфере;
	Знает понятие и особенности информационных систем в банке и других организациях финансовой сферы;
	Знает правовые основы организации защиты конфиденциальной информации;
	Знает основные способы защиты информации;
	Умеет разрабатывать проекты организационно-распорядительных документов, регламентирующих работу по защите информации;
	Умеет выбирать и анализировать методы и средств защиты финансовой информации;

	<p>Определяет виды информации и виды угроз информационной безопасности финансовых организаций;</p> <p>Применяет нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности банков и других организаций финансовой сферы</p>
ПК-2 Способен обеспечивать проведение сделок кредитования корпоративных заёмщиков	
ИПК-2.8 Анализирует базы данных и применяет информационные системы в профессиональной сфере в целях обеспечения информационной безопасности	Знает понятие и виды угроз информационной безопасности в финансовой сфере;
	Знает понятие и особенности информационных систем в банке и других организациях финансовой сферы;
	Знает правовые основы организации защиты конфиденциальной информации
	Знает основные способы защиты информации
	Умеет выбирать и анализировать методы и средств защиты финансовой информации;
	Умеет разрабатывать проекты организационно-распорядительных документов, регламентирующих работу по защите информации
	Определяет виды информации и виды угроз информационной безопасности финансовых организаций;
Применяет нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности банков и других организаций финансовой сферы	
ПК-3 Способен разрабатывать отдельные функциональные направления управления рисками	
ИПК-3.6 Анализирует базы данных и применяет информационные системы в профессиональной сфере в целях обеспечения информационной безопасности	Знает понятие и особенности информационных систем в банке и других организациях финансовой сферы;
	Знает правовые основы организации защиты конфиденциальной информации;
	Знает основные способы защиты информации;
	Знает правовые основы организации защиты конфиденциальной информации;
	Умеет разрабатывать проекты организационно-распорядительных документов, регламентирующих работу по защите информации;
	Умеет выбирать и анализировать методы и средств защиты финансовой информации;
	Определяет виды информации и виды угроз информационной безопасности финансовых организаций;
Применяет нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности банков и других организаций финансовой сферы	

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

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 зачетные единицы (72 часа), их распределение по видам работ представлено в таблице

Виды работ	Всего часов	Форма обучения		
		очная		очно-заочная
		6 семестр (часы)	X семестр (часы)	6 семестр (часы)
Контактная работа, в том числе:		38,2		28,2
Аудиторные занятия (всего):		34		24
занятия лекционного типа		18		12
лабораторные занятия		16		12
практические занятия				

семинарские занятия					
Иная контактная работа:			4,2		4,2
Контроль самостоятельной работы (КСР)			4		4
Промежуточная аттестация (ИКР)			0,2		0,2
Самостоятельная работа, в том числе:			33,8		43,8
Реферат/эссе (подготовка)			10		6
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала НПА и учебных пособий, подготовка к практическим занятиям)			10		7
Подготовка к текущему контролю			13,8		15,8
Контроль:					
Подготовка к экзамену			-		-
Общая трудоемкость	час.	72	72		72
	в том числе контактная работа	38,2	38,2		28,2
	зач. ед	2	2		2

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 6 семестре (*очная форма обучения*)

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1.	Теоретические аспекты информационной безопасности.	8	2		2	4
2.	Понятие и виды защищаемой информации.	17	4		6	7
3.	Понятие и виды угроз информационной безопасности.	8	2		2	4
4.	Методы и средства обеспечения информационной безопасности компьютерных систем.	12	4		2	6
5.	Электронный документооборот и электронная цифровая подпись.	10	2		2	6
6.	Электронные платежные системы и защита банковской информации.	12,8	4		2	6,8
	ИТОГО по разделам дисциплины	67,8	18		16	33,8
	Контроль самостоятельной работы (КСР)	4				
	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

Разделы (темы) дисциплины, изучаемые в 6 семестре (*курсе*) (*очно-заочная форма обучения*)

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1.	Теоретические аспекты информационной безопасности.	11	2		2	7
2.	Понятие и виды защищаемой информации.	14	2		4	8
3.	Понятие и виды угроз информационной безопасности.	8	2			6
4.	Методы и средства обеспечения информационной безопасности компьютерных систем.	12	2		2	8
5.	Электронный документооборот и электронная цифровая подпись.	10	2		2	6
6.	Электронные платежные системы и защита банковской информации.	12,8	2		2	8,8
	ИТОГО по разделам дисциплины	67,8	12		12	43,8
	Контроль самостоятельной работы (КСР)	4	4			
	Промежуточная аттестация (ИКР)	0,2	0,2			
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72	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.	Теоретические аспекты информационной безопасности.	<p>Понятие информационной безопасности. Интересы личности, общества и государства в информационной сфере. Направления и проблемы обеспечения информационной безопасности государства и региональной информационной безопасности.</p> <p>Основные понятия и общеметодологические принципы теории информационной безопасности. Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Принципы информационной безопасности.</p> <p>Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.</p> <p>Информационное противоборство.</p>	Контрольные вопросы
2.	Понятие и виды защищаемой информации.	<p>Понятие и сущность защищаемой информации. Права и обязанности обладателя информации.</p> <p>Виды защищаемой информации: государственная тайна, личная и семейная тайна, профессиональная тайна, служебная тайна, коммерческая тайна, персональные данные. Понятие интеллектуальной собственности и особенности ее защиты.</p> <p>Перечень сведений конфиденциального характера. Банковская, налоговая, страховая, аудиторская и другие виды тайн в финансовой сфере.</p> <p>Правовое регулирование отношений в области обработки персональных данных. Категории ПДн и принципы обработки персональных данных. Права субъектов ПДн и обязанности оператора ПДн при их обработке. Регуляторы в области защиты персональных</p>	Контрольные вопросы

		данных и ответственность за нарушение законодательства о персональных данных.	
3.	Понятие и виды угроз информационной безопасности.	<p>Понятие и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные направления и методы реализации угроз.</p> <p>Компьютерная система как объект информационной безопасности. Неформальная модель нарушителя. Оценка уязвимости системы.</p>	Контрольные вопросы
4.	Методы и средства обеспечения информационной безопасности компьютерных систем.	<p>Общая характеристика способов и средств защиты информации.</p> <p>Правовая, организационная, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.</p> <p>Определение и основные способы несанкционированного доступа.</p> <p>Механизмы защиты информации в автоматизированных системах. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.</p> <p>Краткий анализ моделей и политики безопасности.</p> <p>Политика и модели дискреционного доступа. Парольные системы разграничения. Политика и модели мандатного доступа. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.</p>	Контрольные вопросы
5.	Электронный документооборот и электронная цифровая подпись.	<p>Проблемы информационной безопасности в сфере электронного документооборота.</p> <p>Понятие электронного документа. Федеральный закон РФ «Об электронной цифровой подписи». Российские стандарты ЭЦП (ГОСТ Р 34.10-2012).</p> <p>Электронная цифровая подпись и ее применение. Виды электронных подписей. Формирование и проверка ЭЦП. Методы аутентификации пользователей и документов на основе алгоритма ЭЦП RSA. Методы аутентификации пользователей и документов. Функциональное назначение удостоверяющих центров в системах электронных цифровых подписей.</p>	Контрольные вопросы
6.	Электронные платежные системы и защита банковской информации.	<p>Этапы развития платёжных систем в Интернет. Классификация платежных систем.</p> <p>Платежные системы, построенные на основе понятий «электронные деньги» и «смарт-карты».</p> <p>Средства обеспечения безопасности электронных платежных систем. Обеспечение безопасности в системе интернет-банкинга.</p> <p>Место киберриска в составе основных рисков финансовых организаций.</p> <p>Payment Card Industry Data Security Standard (PCI DSS). Стандарты Банка России (СТО БР ФАПИ.ПАОК-1.0-2021).</p> <p>Деятельность Банка России в области обеспечения киберустойчивости, защиты прав потребителей финансовых услуг, контроля показателей риска информационных угроз в финансовой сфере.</p>	Контрольные вопросы

2.3.2 Занятия семинарского типа (практические /семинарские занятия/ лабораторные работы)

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
1.	Теоретические аспекты информационной безопасности.	Направления и проблемы обеспечения информационной безопасности. Поиск и применение НПА в сфере информационной безопасности. Работа со справочно-информационными правовыми системами.	ЛР, Р, О
2.	Понятие и виды защищаемой информации.	Перечень сведений конфиденциального характера. Банковская, налоговая, страховая, аудиторская и другие виды профессиональных тайн в финансовой сфере. Порядок работы с информацией ДСП. Определение типа информационной системы, актуальных угроз и необходимого уровня защищенности ПДн.	ЛР, Р, Т
3.	Понятие и виды угроз информационной безопасности.	Классификация угроз информационной безопасности. Разработка локальных актов организации по защите информации. Обзор международных стандартов информационной безопасности	ЛР, Р, О
4.	Методы и средства обеспечения информационной безопасности компьютерных систем.	Общая характеристика способов и средств защиты информации. Правовая, организационная, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности. Определение и основные способы несанкционированного доступа. Механизмы защиты информации в автоматизированных системах. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление. Краткий анализ моделей и политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения. Политика и модели мандатного доступа. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.	ЛР, Р, О
5.	Электронный документооборот и электронная цифровая подпись.	Электронная цифровая подпись и ее применение. Виды электронных подписей. Формирование и проверка ЭЦП. Методы аутентификации пользователей и документов на основе алгоритма ЭЦП RSA. Методы аутентификации пользователей и документов на основе алгоритма Эль Гамала. Функциональное назначение удостоверяющих центров в системах электронных цифровых подписей.	ЛР, Р, О
6.	Электронные платежные системы и защита банковской информации.	Место киберриска в составе основных рисков финансовых организаций. Обеспечение безопасности в системе интернет-банкинга. Payment Card Industry Data Security Standard (PCI DSS). Стандарты Банка России (СТО БР ФАПИ.ПАОК-1.0-2021). Деятельность Банка России в области обеспечения киберустойчивости, защиты прав потребителей финансовых услуг, контроля показателей риска информационных угроз.	Опрос, Р, О

Защита лабораторной работы (ЛР), расчетно-графического задания (РГЗ), написание реферата (Р), коллоквиум (К), тестирование (Т) и опрос (О).

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.3 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	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 лабораторных работ	Методические указания по выполнению лабораторных 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
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

В ходе изучения дисциплины «Основы информационной безопасности в финансовой сфере» предусмотрено использование образовательных технологий: лекции, лабораторные работы, проблемное обучение, подготовка письменных аналитических работ, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (мозгового штурма, разбора конкретных ситуаций (кейс-метод) и др.) 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.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Основы информационной безопасности в финансовой сфере».

Оценочные средства включает контрольные материалы для проведения текущего контроля в форме тестовых заданий, доклада-презентации по проблемным вопросам, разноуровневых заданий, ролевой игры, ситуационных задач и промежуточной аттестации в форме вопросов и заданий к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

Код и наименование индикатора	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
		Текущий контроль	Промежуточная аттестация
ИПК-1.9 Анализирует базы данных и применяет информационные системы в профессиональной сфере в целях обеспечения информационной безопасности ИПК-2.8 Анализирует базы данных и применяет информационные системы в профессиональной сфере в целях обеспечения информационной безопасности ИПК-3.6 Анализирует базы данных и применяет информационные системы в профессиональной сфере в целях обеспечения информационной безопасности	Знает понятие и особенности информационных систем в банке и других организациях финансовой сферы;	Реферат Опрос	Вопрос на зачете 2,12-15, 25-30
	Знает правовые основы организации защиты конфиденциальной информации;	Лабораторная работа, Тест	Вопрос на зачете 8-15, 25
	Знает основные способы защиты информации;	Опрос Реферат	Вопрос на зачете 1-6,18-28
	Знает понятие и виды угроз информационной безопасности в финансовой сфере;	Лабораторная работа Опрос по теме	Вопрос на зачете 7-8,16-17,26,29,30
	Умеет выбирать и анализировать методы и средства защиты финансовой информации;	Тест, Лабораторная работа	Вопрос на зачете 2,5, 18-22,27-30
	Умеет разрабатывать проекты организационно-распорядительных документов, регламентирующих работу по защите информации;	Опрос Лабораторная работа Реферат	Вопрос на зачете 12-15,20,25
	Определяет виды информации и виды угроз информационной безопасности финансовых организаций;	Лабораторная работа Опрос	Вопрос на зачете 10-16
	Применяет нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности банков и других организаций финансовой сферы	Опрос Лабораторная работа Реферат	Вопрос на зачете 2-5,29,8-10,19

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 для устного опроса/ дискуссионные вопросы

Тема 1. Теоретические аспекты информационной безопасности.

1. Назовите особенности современного информационного общества.
2. Какие элементы информационной инфраструктуры Вы знаете?
3. Назовите особенности экономической информации.
4. В чем отличия понятий информационный ресурс, продукт и услуга?
5. Что означают конфиденциальность, целостность и доступность информации?
6. Каковы основные принципы построения систем защиты информации?
7. Охарактеризуйте систему органов обеспечения информационной безопасности и защиты информации.
8. Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?
9. Покажите связь между уровнем развития общества и технологиями защиты информации.
10. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
11. С чем связан возросший интерес к проблемам защиты информации?
12. Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
13. Охарактеризуйте понятия, связанные с организацией защиты информации.

Тематика рефератов/докладов-презентаций/индивидуальных заданий

1. Движущие силы и этапы цифровой трансформации общества.
2. Связь цифровых технологий и инноваций.
3. Компьютерные преступления и наказания.
4. Система обеспечения информационной безопасности. Информационное оружие.
5. Управление и защита информации в информационно-телекоммуникационных сетях.
6. Характеристика эффективных стандартов по безопасности. Требования к полноте эффективных стандартов по безопасности.
7. Понятие сквозных технологий и их роль в развитии экономики будущего.
8. Факторы роста спроса на большие данные и мировые тенденции развития технологий big data. Проблема создания и размещения big data-центров.
9. Криптовалюты: специфика, проблемы и перспективы использования.
10. Распределенные вычисления и хранилище данных (облачное хранение)
11. Роль искусственного интеллекта в обработке больших данных и принятии экономических решений. Понятие нейротехнологии.
12. Современные автоматизированные информационные системы в банковском деле (бирже, бюджетных организациях и других финансовых организациях)
13. Обеспечение информационной безопасности кредитной организации.
14. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
15. Порядок защиты информации в рекламной и выставочной деятельности.
16. Порядок подбора персонала организации финансово-кредитной сферы для работы с информацией ограниченного доступа.
17. Методика инструктирования и обучения персонала правилам защиты информации ограниченного доступа.
18. Анализ международных стандартов информационной безопасности.

Тест

По теме 2: Понятие и виды защищаемой информации.

Вариант 1

А. Подберите правильное определение

1. Персональные данные

2. Врачебная тайна

<http://semeynoepravo.com/pasport/biometricheskie-personalnye-dannye.html>

3. Коммерческая тайна

4. Секрет производства

5. Банковская тайна

6. Профессиональная тайна

7. Служебная тайна

- а) информация о состоянии здоровья, диагнозе, результатах обследования и сведений о личной жизни, полученных при обследовании и лечении ;
- б) сведения любого характера о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную ценность вследствие неизвестности их третьим лицам;
- в) группа охраняемых законом тайн, необходимость соблюдения которых вытекает из доверительного характера определенных видов деятельности
- г) сведения о счетах, взносах, операциях, личности клиентов кредитной организации, корреспондентов и лиц, упомянутых в договорах с ней;
- д) сведения, полученные или разработанные гос.органами и органами местного самоуправления на законном основании, ограничение доступа к которым введено для обеспечения информационной безопасности управленческой деятельности государственных и муниципальных органов
- е) режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную выгоду;
- ж) любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу

В. Укажите виды информации, относящиеся и не относящиеся к коммерческой тайне

1. Не относится к коммерческой тайне

а) Информация, содержащаяся в документах (лицензии), дающих право на осуществление предпринимательской деятельности;

б) Базы данных клиентов и контрагентов

в) Сведения о размерах и структуре доходов и расходов некоммерческих организаций, размере и составе их имущества;

2. Является коммерческой тайной

г) Сведения о методах расчета и структуре выходных цен, о размерах предоставляемых скидок ;

д) Информация о об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
е) Содержание первичных документов и регистров бухгалтерского учета, кроме бухгалтерских сведений, которые содержатся в открытых источниках;
ж) Сведения о результатах финансового мониторинга в отношении организаций и физ. лиц, полученных в связи с проверкой их причастности к террористической деятельности

С. Заполните пропуски

а) В правом верхнем углу первой страницы документа для служебного пользования, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам проставляются.....

б) Проверка наличия документов, дел и изданий с пометкой "Для служебного пользования" проводится не реже

в) На каждый утраченный документ ДСП составляют

г) За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, служащий (работник) несет.....ответственность

Лабораторная работа № 1

Работа со справочно-информационными правовыми системами

Цель работы: приобретение практических навыков поиска НПА и работы с информационно-правовыми системами по вопросам защиты информации в финансовой сфере.

Задание:

1) Проверить представленные документы на предмет их соответствия и действия по состоянию текущую дату.

2) Расположить их по степени важности и принадлежности к правовым группам (видам нормативного акта).

3) Указать документы, утратившие силу.

4) Дополнить список документами, не включёнными в перечень, необходимыми при изучении вопросов Информационной безопасности.

5) Составить схему (интеллект-карту) иерархии НПА в области информационной безопасности в финансовой сфере.

Порядок работы:

Запустить справочно-правовую систему «КонсультантПлюс».

Ознакомиться со структурой и возможностями Стартового окна.

Войти из Стартового окна в режим «Обзоры». Просмотреть всю информацию в разделе: Правовые новости.

Из Стартового окна перейти в раздел «Законодательство». Ознакомиться с общим построением справочно-информационной правовой системы «КонсультантПлюс».

Изучить поочередно все подпункты основного меню системы. Зайти в «Карточку поиска», рассмотреть все её элементы.

Зайти в режим Правового навигатора. Изучить: особенности поиска информации по конкретному правовому вопросу; двухуровневую структуру словаря; ключевые понятия и группы ключевых понятий; различные виды сортировки списка.

Найти нормативно-правовые документы, используя различные виды поиска.

Изучить самостоятельно возможности СПС «Гарант».

Приложение 1

Перечень документов:

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
2. Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.
3. Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента Российской Федерации от 12 мая 2009 г. № 537.
4. Основы организации защиты информации в Приволжском федеральном округе (Одобрены Решением Координационного Совета по защите информации при полномочном представителе Президента Российской Федерации в Приволжском федеральном округе от 12 ноября 2009 года).
5. Конституция Российской Федерации.
6. Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ «О безопасности».
7. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
8. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»
9. «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утверждено постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 г. № 912-51.
10. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
11. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
12. Указ Президента Российской Федерации от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена".
13. Приказ Федеральной службы охраны Российской Федерации от 7.08.2009 № 487 «Об утверждении положения о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации».
14. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
15. Федеральный закон РФ от 29 июля 2004 г № 98-ФЗ «О коммерческой тайне».
16. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».
17. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности»
18. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
19. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

1. Понятие информационной безопасности.
2. Особенности обеспечения информационной безопасности в финансовой сфере.
3. Основные понятия и общеметодологические принципы теории информационной безопасности. Источники понятий в области информационной безопасности.
4. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации.

5. Принципы информационной безопасности.
6. Органы обеспечения информационной безопасности и защиты информации в РФ, их функции и задачи, нормативная деятельность.
7. Информационные войны и информационное противоборство.
8. Понятие правонарушений в информационной сфере.
9. Ответственность за правонарушения в информационной сфере.
10. Понятие и виды защищаемой информации.
11. Сведения, составляющие государственную тайну, их засекречивание и рассекречивание. Защита сведений, составляющих государственную тайну.
12. Понятие и виды профессиональных тайн.
13. Служебная тайна. Особенности работы с информацией ДСП.
14. Понятие коммерческой тайны. Отнесение информации к информации, составляющей коммерческую тайну.
15. Понятие и виды персональных данных. Принципы обработки персональных данных.
16. Понятие и виды угроз информационной безопасности.
17. Оценка уязвимости системы.
18. Общая характеристика способов и средств защиты информации.
19. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно- аппаратные средства обеспечения информационной безопасности.
20. Механизмы защиты информации в автоматизированных системах.
21. Основные модели и политики безопасности.
22. Популярные антивирусные программы и их классификация.
23. Понятие и виды электронной подписи.
24. Правовой статус удостоверяющего центра. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи.
25. Деятельность Банка России в области обеспечения киберустойчивости, защиты прав потребителей финансовых услуг, контроля показателей риска информационных угроз в финансовой сфере.
26. Классификация платежных систем и угроз для них.
27. Обеспечение безопасности в системе интернет-банкинга.
28. Биометрические системы идентификации
29. Аудит ИБ автоматизированных банковских систем.
30. Понятие и место киберриска в составе основных рисков финансовых организаций.

Критерии оценивания результатов обучения

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает сущность информационной безопасности и методы обеспечения информационной безопасности в финансовой сфере, допускает незначительные ошибки; студент применяет нормативно-правовую базу в конкретных практических ситуациях.

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры налоговых рисков, 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

Основная литература:

1. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978-5-8114-7338-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/158939> — Режим доступа: для авториз. пользователей.

2. Информационная безопасность: Учебное пособие для студентов, обучающихся по направлению подготовки 38.03.01 «Экономика»/ Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. - Под общ. ред. проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017 – 198 с. [Электронный ресурс] Режим доступа: <infbezop.pdf> (<yandex.ru>)

3. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/156401> — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 N 646

2. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 N 203;

3. Стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0[Электронный ресурс] Режим доступа: https://cbr.ru/information_security/Gubzi_docs/

4. Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш . - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. - Режим доступа: <http://znanium.com/catalog.php?bookinfo=763644>.

5. Партыка Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2019. - 432 с. [Электронный ресурс] Режим доступа: <https://new.znaniyum.com/catalog/product/987326> (дата обращения: 30.01.2020); для авториз. пользователей. - ISBN 978-5-16-101302-1.

5.2. Периодическая литература

Журнал «Информатизация и связь»

Базы данных компании «Ист Вью» <http://dlib.eastview.com>

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.znaniyum.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 Wiley <https://onlinelibrary.wiley.com/>
5. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН <http://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. Ельцина <https://www.prlib.ru/>
9. zbMath <https://zbmath.org/>
10. Nano Database <https://nano.nature.com/>
11. Springer eBooks: <https://link.springer.com/>
12. "Лекториум ТВ" <http://www.lektorium.tv/>
13. 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 ресурсов <http://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 словарей <http://www.glossary.ru/>;
12. Словари и энциклопедии <http://dic.academic.ru/>;
13. Образовательный портал "Учеба" <http://www.uceba.com/>;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы

КубГУ:

1. Среда модульного динамического обучения <http://moodle.kubsu.ru>
2. База учебных планов, учебно-методических комплексов, публикаций и конференций <http://mschool.kubsu.ru/>
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий <http://mschool.kubsu.ru>;
4. Электронный архив документов КубГУ <http://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)

Изучение дисциплины «Основы информационной безопасности в финансовой сфере» предусматривает чтение лекций, проведение практических занятий, самостоятельную работу студентов.

В ходе лекций раскрываются основные теоретические, правовые и методические вопросы защиты информации в интересах потребителей финансовых услуг и финансово-кредитной сферы. Используются интерактивные методы обучения – проблемные лекции, лекции-дискуссии. Материал лекции излагается с учетом принципа наглядности обучения в виде презентации с использованием мультимедийной аппаратуры. Материалы лекций являются основой для подготовки студента к лабораторным работам и выполнения заданий самостоятельной работы.

Основной целью практических занятий является разбор практических ситуаций. Выполнение лабораторных работ, а также текущий контроль усвоения пройденного материала. Проводится экспресс-опрос по изучаемой теме, обсуждение актуальных или сложных вопросов. Практические занятия проводятся с использованием интерактивных технологий в виде заданий на базе реальных ситуаций, обсуждения и проведения дискуссий по наиболее актуальным проблемам.

Студент может в достаточном объеме усвоить и успешно реализовать конкретные знания, умения, навыки и компетенции в своей практической деятельности при выполнении следующих условий:

- 1) систематическая работа на учебных занятиях под руководством преподавателя и самостоятельная работа по закреплению полученных знаний и навыков;
- 2) добросовестное выполнение заданий;
- 3) выяснение и уточнение отдельных предпосылок, умозаключений и выводов, содержащихся в учебном курсе; взаимосвязей отдельных его разделов, используемых методов, характера их использования в практической деятельности;
- 4) сопоставление определений, методик, по затрагиваемым в учебном курсе проблемам; выявление особенностей их применения в финансовой сфере;
- 5) подготовка научных статей для опубликования в периодической печати,

выступление на научно-практических конференциях, участие в работе студенческих научных обществ, круглых столах и диспутах.

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-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

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	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютеры, ноутбуки	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Лаборатория информационных и управляющих систем 201Н	Оборудование: ПК, Терминальные станции, Усилитель автономный беспроводной	1С: Предприятие 8 SPSS Statistics
Лаборатория экономической информатики 202Н		Microsoft Windows 8, 10, Microsoft Office Professional Plus
Лаборатория экономики и управления 212Н	Многофункциональный профессиональный видео детектор банкнот и ценных бумаг, Счетчики банкнот, Инфракрасный детектор банкнот и ценных бумаг, Универсальный детектор банкнот и ценных бумаг, Детектор подлинности банкнот, Ящик денежный, Планшетный импринтер, Усилитель автономный беспроводной	Microsoft Windows 8, 10, Microsoft Office Professional Plus

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)	<p>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)</p>	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Помещение для самостоятельной работы обучающихся (ауд.213 А, 218 А)	<p>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)</p>	Microsoft Windows 8, 10, Microsoft Office Professional Plus