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 - первый
проректор
_____ Т.А. Хагуров
подпись
«26» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Б1.В.ДЭ.01.01 КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСОВОЙ СФЕРЕ

Направление подготовки/специальность 38.04.08 Финансы и кредит

Направленность (профиль) / специализация Финансы в цифровой экономике

Форма обучения очная, заочная

Квалификация Магистр

Краснодар 2023

Рабочая программа дисциплины «Кибербезопасность в финансовой сфере» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 38.04.08 Финансы и кредит

Программу составил (и):
И.В. Савельев, канд. технич. наук, доцент

А.И. Бабенко, преподаватель

Рабочая программа дисциплины «Кибербезопасность в финансовой сфере» утверждена на заседании кафедры экономического анализа, статистики и финансов протокол № 6 от 3 мая 2023 г.

Заведующий кафедрой экономического анализа, статистики и финансов

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

Утверждена на заседании учебно-методической комиссии экономического факультета протокол № 7 от 16 мая 2023 г.

Председатель УМК факультета
Л.Н. Дробышевская
доктор экон. наук, профессор

Рецензенты:

Гайденко В.В., канд. экон. наук, доцент кафедры бухгалтерского учета, аудита и автоматизированной обработки данных ФГБОУ ВО «Кубанский государственный университет»
Бутренин А.А., канд. экон. наук, директор ООО «Ваш Актив»

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Целью освоения дисциплины является применение на основе анализа киберугроз приёмов и методов, повышающих уровень кибербезопасности при осуществлении корпоративного кредитования и финансового консультирования.

1.2 Задачи дисциплины

Исходя из определённой цели задачами дисциплины являются:

- изучение классификации киберугроз, присущих финансовой сфере;
- анализ состояния уровня кибербезопасности операций, осуществляемых финансово-кредитными организациями;
- приобретение практики использования приёмов и методов, повышающих уровень кибербезопасности в рамках финансового консультирования и корпоративного кредитования.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Кибербезопасность в финансовой сфере» относится к элективным дисциплинам (модулям) 1 учебного плана. В соответствии с рабочим учебным планом дисциплина изучается на 2 курсе по очной и на 2 курсе по заочной форме обучения. Вид промежуточной аттестации: зачет.

Изучение данной дисциплины основывается на знаниях и практических навыках, приобретённых при изучении таких дисциплин как «Информационно-аналитические системы и технологии в финансовой сфере», «Системы искусственного интеллекта», «Технологии корпоративного кредитования». В соответствии с учебным планом, знания и практические навыки, полученные при изучении данной дисциплины, могут быть использованы при изучении таких дисциплин как «Финансовые технологии» и «Финансовое консультирование».

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-3 Способен консультировать партнёров, клиентов и контрагентов при проведении кредитных сделок	
ИПК-3.1 Демонстрирует способность готовить аналитическое обоснование сделок корпоративного кредитования и проводить консультирование руководителей различных уровней	Знает основы обеспечения информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасностью
	Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет использовать информационные технологии в процессе корпоративного кредитования
	Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования Использует информационные технологии в процессе корпоративного кредитования
ИПК-3.2 Анализирует мотивационные программы и программы лояльности при продвижении программ корпоративного кредитования	Знает основы обеспечения информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
	управления информационными технологиями и информационной безопасностью
	Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет использовать информационные технологии в процессе корпоративного кредитования
	Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования Использует информационные технологии в процессе корпоративного кредитования
ПК-4 Способен управлять процессом финансового планирования и консультирования	
ИПК-4.1 Применяет методы финансового планирования и консультирования	Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями Знает основные положения национальных и международных стандартов и руководств по информационной безопасности
	Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет использовать информационные технологии в процессе корпоративного кредитования
	Организует консультационную поддержку по вопросам аппаратно-информационного обеспечения Использует информационные технологии в процессе финансового планирования и консультирования
ПК-5 Способен управлять корпоративным кредитным портфелем	
ИПК-5.1 Применяет инструментарий управления выполнением плана продаж кредитных продуктов корпоративным клиентам	Знает общие вопросы информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасностью
	Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет применять информационными технологии при корпоративном кредитовании обеспечивая информационную безопасность
	Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования Использует информационные технологии в процессе корпоративного кредитования
ИПК-5.2 Демонстрирует способность разрабатывать предложения по совершенствованию бизнес-процессов корпоративного кредитования	Знает общие вопросы информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасностью
	Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет применять информационными технологии при корпоративном кредитовании обеспечивая информационную безопасность

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
	Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования; Использует информационные технологии в процессе корпоративного кредитования
ИПК-5.4 Применяет инструментарий управления кредитными рисками портфеля корпоративных кредитов	Знает общие вопросы информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасностью
	Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет применять информационные технологии при управлении кредитными рисками
	Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования Использует информационные технологии, применяемые в процессе управления кредитным риском портфеля корпоративных кредитов

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 зачетных единиц (72 часа), их распределение по видам работ представлено в таблице

Виды работ	Всего часов	Форма обучения	
		очная	заочная
		4 семестр (часы)	2 курс (часы)
Контактная работа, в том числе:			
Аудиторные занятия (всего):		**24**	**12**
занятия лекционного типа		8	4
практические занятия		16	8
Иная контактная работа:			
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе:		**47,8**	**56**
Расчётно-графическая работа (РГР) (подготовка)		30	40
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям)		10	10
Подготовка к текущему контролю		7,8	6
Контроль:			
Подготовка к зачёту		-	3,8

Общая трудоемкость	**час.**		**72**	**72**
	в том числе контактная работа		**24,2**	**12.2**
	зач. ед.		**2**	**2**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 4 семестре (**очная** форма обучения)

№	Наименование разделов (тем)	Количество часов			
		Всего	Аудиторная работа		Внеаудиторная работа
			Л	ПЗ	СРС
1.	Киберугрозы в финансовой сфере	14	2	2	10
2.	Типовые уязвимости в системах киберзащиты	18	2	6	10
3.	Основные направления обеспечения кибербезопасности в финансовой сфере	32	4	8	20
	ИТОГО по разделам дисциплины		8	16	40
	Промежуточная аттестация (ИКР)	0,2			
	Подготовка к текущему контролю				7,8
	Общая трудоемкость по дисциплине	72			

Примечание: Л – лекции, ПЗ – практические занятия, СРС – самостоятельная работа студента

Разделы (темы) дисциплины, изучаемые на 2 курсе (**заочная** форма обучения)

№	Наименование разделов (тем)	Количество часов			
		Всего	Аудиторная работа		Внеаудиторная работа
			Л	ПЗ	СРС
1.	Киберугрозы в финансовой сфере	18	1	2	15
2.	Типовые уязвимости в системах киберзащиты	18	1	2	15
3.	Основные направления обеспечения кибербезопасности в финансовой сфере	26	2	4	20
	ИТОГО по разделам дисциплины		4	8	50
	Контроль самостоятельной работы (КСР)	3,8			
	Промежуточная аттестация (ИКР)	0,2			
	Подготовка к текущему контролю				6
	Общая трудоемкость по дисциплине	72			

Примечание: Л – лекции, ПЗ – практические занятия / семинары, 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.	Киберугрозы в финансовой сфере	Стандарты кибербезопасности. Классификация типов киберпреступлений согласно Конвенции Совета Европы. Киберпреступления и киберпреступники в финансовой сфере: классификация, методы действия и способы защиты. Легализация бизнеса по разработке шпионских программ как новая угроза кибербезопасности.	Контрольные вопросы (КВ), тесты (Т)
2.	Типовые уязвимости в системах киберзащиты	Методы выявления программных уязвимостей Антивирусные программы. Проактивная антивирусная защита – функции и возможности. Иммунный подход к защите информационных систем. Классификация, способы и объекты кибершпионажа. Кибербразведка и контрразведка: цели, задачи и методы работы. Методологические особенности отбора и подготовки специалистов в области кибербразведки и	Контрольные вопросы (КВ), тесты (Т)

		киберконтрразведки. Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем. Базовые термины и определения кибербезопасности. Редтайминг и блютайминг	
3.	Основные направления обеспечения кибербезопасности в финансовой сфере	База знаний MITRE ATT&CK. SIEM как важный элемент в архитектуре киберзащиты. Магический квадрат Gartner. Типовые атаки на организации кредитно-финансовой сферы при корпоративном кредитовании и финансовом консультировании. Атаки с применением методов социальной инженерии в отношении сотрудников банка. Атаки на системы дистанционного банковского обслуживания, используемые юридическими лицами. Атаки на клиентов – физических лиц. Атаки на устройства самообслуживания (отмена транзакции). Электронный банкинг и риски недостаточного обеспечения информационной безопасности. Кибербезопасность в условиях применения систем электронного банкинга. Влияние теневого интернета на безопасность электронного банкинга	Контрольные вопросы (КВ), тесты (Т)

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

№	Наименование раздела (темы)	Тематика практических занятий	Форма текущего контроля
1.	Киберугрозы в финансовой сфере	Составьте классификацию киберугроз, связанных с деятельностью финансово-кредитных организаций. Согласно этой классификации ранжируйте опасности киберпространства для выбранной организации финансово-кредитной сферы, сделав акцент на операциях, связанных с корпоративным кредитованием и финансовым консультированием.	РГЗ
2.	Типовые уязвимости в системах киберзащиты	Для анализируемой организации выделите типовые уязвимые места в киберзащите, предложите инструментарий для улучшения состояния киберзащиты организации	*РГЗ*
3.	Основные направления обеспечения кибербезопасности в финансовой сфере	Оцените возможные затраты на улучшение киберзащиты, определите очерёдность мероприятий и степень их эффективности для организации, выполняющим операции по корпоративному кредитованию и финансовому консультированию	РГЗ

При изучении дисциплины могут применятся 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

№	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	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
3	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

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 предусмотрено использование следующих образовательных технологий: лекции, практические занятия и самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий 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 «Кибербезопасность в финансовой сфере».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме контрольных вопросов (КВ), тестов (Т) и **промежуточной аттестации** в форме вопросов к зачёту.

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)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИПК-3.1 Демонстрирует способность готовить аналитическое обоснование сделок корпоративного кредитования и проводить консультирование	Знает основы обеспечения информационной безопасности банка Знает основные положения национальных и международных	Контрольные вопросы (КВ), тесты (Т)	Вопрос на зачёте 1-5

	руководителей различных уровней	стандартов и руководств в области управления информационными технологиями и информационной безопасностью		
		Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет использовать информационные технологии в процессе корпоративного кредитования		
		Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования Использует информационные технологии в процессе корпоративного кредитования		
2	ИПК-3.2 Анализирует мотивационные программы и программы лояльности при продвижении программ корпоративного кредитования	Знает основы обеспечения информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасностью	Контрольные вопросы (КВ), тесты (Т)	Вопрос на зачёте 6-10
		Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет использовать информационные технологии в процессе корпоративного кредитования		
		Организует аппаратно-информационное		

		обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования Использует информационные технологии в процессе корпоративного кредитования		
3	ИПК-4.1 Применяет методы финансового планирования и консультирования	Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями Знает основные положения национальных и международных стандартов и руководств по информационной безопасности	Контрольные вопросы (КВ), тесты (Т)	Вопрос на зачёте 11-15
		Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет использовать информационные технологии в процессе корпоративного кредитования		
		Организует консультационную поддержку по вопросам аппаратно-информационного обеспечения Использует информационные технологии в процессе финансового планирования и консультирования		
4	ИПК-5.1 Применяет инструментарий управления выполнением плана продаж кредитных продуктов корпоративным клиентам	Знает общие вопросы информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области управления информационными	Контрольные вопросы (КВ), тесты (Т)	Вопрос на зачёте 16-20

		технологиями и информационной безопасностью Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет применять информационными технологии при корпоративном кредитовании обеспечивая информационную безопасность Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования Использует информационные технологии в процессе корпоративного кредитования		
5	ИПК-5.2 Демонстрирует способность разрабатывать предложения по совершенствованию бизнес-процессов корпоративного кредитования	Знает общие вопросы информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасностью Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет применять информационными технологии при корпоративном кредитовании обеспечивая информационную безопасность	Контрольные вопросы (КВ), тесты (Т)	Вопрос на зачёте 21-24

		Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования; Использует информационные технологии в процессе корпоративного кредитования		
6	ИПК-5.4 Применяет инструментарий управления кредитными рисками портфеля корпоративных кредитов	Знает общие вопросы информационной безопасности банка Знает основные положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасностью	Контрольные вопросы (КВ), тесты (Т)	Вопрос на зачёте 25-30
		Умеет обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности Умеет применять информационные технологии при управлении кредитными рисками		
		Организует аппаратно-информационное обеспечение и обеспечение информационной безопасности в сфере корпоративного кредитования и финансового консультирования Использует информационные технологии, применяемые в процессе управления кредитным риском портфеля корпоративных кредитов		

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

Примеры тестов (Т) по разделу 1 «Киберугрозы в финансовой сфере»

1. Основными источниками угроз кибербезопасности являются: а) хищение жёстких дисков, подключение к сети, инсайдерство; б) перехват данных, хищение данных, изменение архитектуры системы; в) хищение данных, подкуп системных администраторов, нарушение регламента работы.

2. Видами кибербезопасности являются: а) персональная, корпоративная, государственная; б) клиентская, серверная, сетевая; в) локальная, глобальная, смешанная.

3. Основными объектами кибербезопасности являются: а) компьютерные сети, базы данных; б) информационные системы, психологическое состояние пользователей; в) бизнес-ориентированные, коммерческие системы.

4. Основными рисками кибербезопасности являются: а) искажение, уменьшение объёма, перекодировка информации; б) техническое вмешательство, выведение из строя оборудования сети; в) потеря, искажение, утечка информации.

5. К основным принципам обеспечения кибербезопасности относятся: а) экономической эффективности системы безопасности; б) многоплатформенной реализации системы; в) усиления защищённости всех звеньев системы.

6. Наиболее распространены угрозы кибербезопасности корпоративной системы в финансовой сфере: а) покупка нелицензионного программного обеспечения; б) ошибки эксплуатации и неумышленного изменения режима работы системы; в) сознательного внедрения сетевых вирусов.

Примеры контрольных вопросов (КВ) по разделу 2 «Типовые уязвимости в системах киберзащиты»

1. Назовите направления целевых кибератак на финансово-кредитные организации
2. В чём сущность кибератаки с применением методов социальной инженерии в отношении сотрудников банка?
3. Как проявляется кибератаки на системы дистанционного банковского обслуживания, используемые юридическими лицами?
4. Как обнаружить кибератаку на клиентов – физических лиц?
5. Чем опасны кибератаки на устройства самообслуживания (отмена транзакции)?

Примерное содержание расчётно-графического задания по разделу 3 «Основные направления обеспечения кибербезопасности в финансовой сфере»

Оцените возможные киберугрозы и степень киберзащищённости анализируемой организации финансово-кредитной сферы. Представьте в виде диаграммы киберугрозы, рассчитайте показатели, характеризующие состояние киберзащиты в организации.

Сформулируйте предложения по повышению эффективности киберзащиты организации, оцените связанные с этими мероприятиями затраты.

Зачётно-экзаменационные материалы для промежуточной аттестации (зачёт)

Перечень вопросов для промежуточной аттестации (зачёт)

1. Общее понятие о кибербезопасности. Кибертерроризм и киберпреступность.
2. Стандарты кибербезопасности. Классификация типов киберпреступлений согласно Конвенции Совета Европы.
3. Киберпреступления и киберпреступники: классификация, методы действия и способы защиты.
4. Легализация бизнеса по разработке шпионских программ как новая угроза кибербезопасности.

5. Краткая история развития кибероружия
6. Методологические принципы классификации кибероружия
7. Проблемы идентификации исполнителей и заказчиков кибератак
8. Типовые уязвимости в системах киберзащиты
9. Методы выявления программных уязвимостей
10. Антивирусные программы
11. Проактивная антивирусная защита – функции и возможности
12. Иммунный подход к защите информационных систем
13. Классификация, способы и объекты кибершпионажа
14. Кибербразведка и контрразведка: цели, задачи и методы работы
15. Методологические особенности отбора и подготовки специалистов в области кибербразведки и киберконтрразведки
16. Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем
17. Базовые термины и определения кибербезопасности
18. Редтайминг и блютайминг
19. Охота за угрозами как проактивный метод киберзащиты
20. База знаний MITRE ATT&CK
21. SIEM как важный элемент в архитектуре киберзащиты
22. Магический квадрат Gartner
23. Типовые атаки на организации кредитно-финансовой сферы при корпоративном кредитовании и финансовом консультировании
24 Атаки с применением методов социальной инженерии в отношении сотрудников банка
25. Атаки на системы дистанционного банковского обслуживания, используемые юридическими лицами
26. Атаки на клиентов – физических лиц
27. Атаки на устройства самообслуживания (отмена транзакции)
28. Электронный банкинг и риски недостаточного обеспечения информационной безопасности
29. Кибербезопасность в условиях применения систем электронного банкинга
30. Влияние теневого интернета на безопасность электронного банкинга

Критерии оценивания по зачёту:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает сущность и основные термины кибербезопасности допускает незначительные ошибки; студент умеет правильно объяснять значение кибербезопасности для сферы корпоративного кредитования и финансового консультирования, иллюстрируя его примерами использования методов киберзащиты для организаций финансово-кредитной сферы.

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры по классификации киберугроз, демонстрирует довольно ограниченный объем знаний программного материала по методам киберзащиты.

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.Защита информации: учебное пособие для вузов/А.А.Внуков. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2021. – 161 с. https://urait.ru/viewer/zaschita-informacii-470131.

2.Кибербезопасность в условиях электронного банкинга: практическое пособие/Под ред. П.В.Ревенкова. – Москва: Прометей, 2020. -522 с. https://znanium.com/read?id=374846.

3. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения/А.И.Белоус, В.А.Солодуха. – Москва: Техносфера, 2021. – 482 с. https://biblioclub.ru/index.php?page=book_view_red&book_id=617523.

5.2. Периодическая литература

1. Журнал «Национальная безопасность» https://www.kubsu.ru/ru/node/15554

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. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
5. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru

6. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
7. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
8. Springer Materials http://materials.springer.com/
9. Nano Database https://nano.nature.com/
10. "Лекториум ТВ" http://www.lektorium.tv/
11. 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. КиберЛенинка (http://cyberleninka.ru/);
2. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
3. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
4. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
5. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
6. Служба тематических толковых словарей http://www.glossary.ru/;
7. Словари и энциклопедии http://dic.academic.ru/;
8. Образовательный портал "Учеба" http://www.ucheba.com/;
9. 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

Самостоятельная работа студентов является важной составной частью процесса обучения. Такая работа должна содействовать более глубокому освоению изучаемого материала, формировать навыки исследовательской работы и ориентировать обучающихся на умение применять на практике теоретические знания.

Самостоятельная работа предполагает детальное изучение лекционного материала, подготовку к практическим занятиям, определение возможности применения полученных знаний для подготовки тезисов докладов на научно-практические конференции, статей, ознакомление с Интернет-ресурсами по тематике изучаемой дисциплины, а также подготовку к промежуточной аттестации в виде зачёта.

Основной теоретический материал даётся магистрантам в виде лекций с презентациями.

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

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

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	Microsoft Windows 8, 10, Microsoft Office Professional Plus

	оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	