Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по учебной работе
к.э.н., доцент Изместьев А.А

17.06.2019г.

Рабочая программа дисциплины
Б1.ДВ.18. Кибербезопасность финансово-кредитных организаций

Направление подготовки: 38.03.01 Экономика
Направленность (профиль): Финансы и кредит, бухгалтерский учет и налогообложение
Квалификация выпускника: бакалавр
Форма обучения: очная, заочная

	Очная ФО	Заочная ФО
Курс	4	4
Семестр	42	42
Лекции (час)	14	4
Практические (сем, лаб.) занятия (час)	14	10
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	80	94
Курсовая работа (час)		
Всего часов	108	108
Зачет (семестр)		
Экзамен (семестр)	42	42

Иркутск 2019

Программа составлена в соответствии с ФГОС ВО по направлению 38.03.01 Экономика.

Автор М.Г. Жигас

Рабочая программа обсуждена и утверждена на заседании кафедры финансов и финансовых институтов

Заведующий кафедрой Т.В. Щукина

Дата актуализации рабочей программы: 30.06.2020
Дата актуализации рабочей программы: 30.06.2021
Дата актуализации рабочей программы: 30.06.2022

1. Цели изучения дисциплины

- приобретение знаний о месте и роли защиты информации в общей системе безопасности и в финансово-кредитных организациях;
- формирование знаний и умений, связанных с содержанием мероприятий по защите информации и оценке рисков кибербезопасности;
- освоение направлений правового регулирования в сфере защиты информации в области финансов и кредита, в том числе с учетом международной практики;
- формирование умений формального представления моделей безопасности финансово-кредитных организаций для (управления доступом, т. д.).
- формирование навыков оценки информационной безопасности и определения информационных рисков, рисков киберугроз

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

Компетенции обучающегося, формируемые в результате освоения дисциплины

Код компетенции по ФГОС ВО	Компетенция
ПК-5	способность анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в отчетности предприятий различных форм собственности, организаций, ведомств и т. д. и использовать полученные сведения для принятия управленческих решений
ПК-10	способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Структура компетенции

Компетенция	Формируемые ЗУНы
ПК-5 способность анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в отчетности предприятий различных форм собственности, организаций, ведомств и т. д. и использовать полученные сведения для принятия управленческих решений	З. Знать основные направления анализа информации бухгалтерской (финансовой) отчетности У. Уметь рассчитывать основные показатели финансового состояния по данным бухгалтерской (финансовой) отчетности организаций, ведомств, предприятий различных форм собственности и интерпретировать полученные результаты Н. Владеть навыком принятия управленческих решений на основе анализа информации, содержащейся в бухгалтерской (финансовой) отчетности
ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии	З. Знать основные принципы использования современных технических средств и информационных технологий, используемых для целей коммуникации У. Уметь осуществлять коммуникации с использованием современных технических средств и информационных технологий Н. Владеть навыком решения коммуникатиных задач посредством технических средств с использованием информационных технологий

3. Место дисциплины (модуля) в структуре образовательной программы

Принадлежность дисциплины - БЛОК 1 ДИСЦИПЛИНЫ (МОДУЛИ): Дисциплина по выбору.

Предшествующие дисциплины (освоение которых необходимо для успешного освоения данной): "Информационные технологии", "Финансы", "Бизнес-аналитика"

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зач. ед.,108 часов.

Вид учебной работы	Количество часов (очная ФО)	Количество часов (заочная ФО)
Контактная(аудиторная) работа		
Лекции	14	4
Практические (сем, лаб.) занятия	14	10
Самостоятельная работа, включая подготовку к экзаменам и зачетам	80	94
Всего часов	108	108

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Содержание разделов дисциплины

Заочная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Развитие информационного общества и информационная безопасность, кибербезопасность	42	0	2	20		1. 2
2	Общее подходы и мероприятия по защите информации и кибербехопасности в финансово-кредитных организациях Правовое регулирование в сфере защиты информации Анализ информационных	42	0	2	10		

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
	рисков Инструментальные средства анализа информационных рисков						
3	Меры и средства обеспечения свойств информационной кибербезопасности в финансовом секторе	42	4	2	24		3
4	Правовое регулирование в сфере защиты информации	42	0	2	20		
5	Анализ информационных рисков в финансово-кредитных организациях	42	0	2	20		4
	ИТОГО		4	10	94		

Очная форма обучения

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
1	Развитие информационного общества и информационная безопасность, кибербезопасность	42	2	3	20		1. 2
2	Общее подходы и мероприятия по защите информации и кибербехопасности в финансово-кредитных организациях Правовое регулирование в сфере защиты информации Анализ информационных рисков Инструментальные средства анализа информационных рисков	42	3	2	10		
3	Меры и средства	42	3	3	10		3

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
	обеспечения свойств информационной кибербезопасности в финансовом секторе						
4	Правовое регулирование в сфере защиты информации	42	3	3	20		
5	Анализ информационных рисков в финансово-кредитных организациях	42	3	3	20		4
	ИТОГО		14	14	80		

5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1		Понятие и сущность защиты информации. Цели защиты информации. Концептуальная модель информационной безопасности. Предмет защиты информации. Информация как объект права собственности. Объект защиты информации. Угрозы информационной безопасности: случайные и преднамеренные. Модель гипотетического нарушителя информационной безопасности. Системное обеспечение защиты информации. Основные принципы построения системы защиты. Методы защиты информации. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Организационные меры и меры обеспечения физической безопасности.
1		Идентификация и аутентификация. Разграничение доступа. Криптографические методы обеспечения конфиденциальности информации. Методы защиты внешнего периметра. Протоколирование и аудит. Построение систем защиты от угроз нарушения целостности. Принципы обеспечения целостности. Криптографические методы обеспечения целостности информации. Построение систем защиты от угроз нарушения доступности. Минимизация ущерба от аварий и стихийных бедствий. Повышение надежности информационной системы. Создание отказоустойчивых информационных систем. Оптимизация взаимодействия пользователей и обслуживающего персонала. Модели защиты информации.
2		Основные определения. Монитор безопасности обращений. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом. Скрытые каналы

№ п/п	Наименование разделов и тем	Содержание
		передачи информации.
3		Информация как объект преступных посягательств. Система правоохранительных органов РФ, связанных с информационной сферой. Понятие компьютерных преступлений и их классификация. Субъект преступлений в сфере компьютерной информации: особенности. Преступления, совершенные с помощью компьютера и их особенности. Основы расследования компьютерных преступлений. Доказательства и доказывание. Международное право при компьютерных инцидентах. Нормы уголовного права некоторых зарубежных стран. Правовые документы по информационной безопасности. Технические документы по информационной безопасности.
4		Аналитический обзор инструментальных средств для анализа рисков и защищенности корпоративных систем Intranet/Internet. Инструментальные проверки уровня безопасности. Internet Scanner и System Security Scanner. Сканер уязвимости Symantec NetRecon. Система централизованного управления безопасностью Enterprise Security Manager. Сканер уязвимости системы безопасности Cisco Secure Scanner (NetSonar). Сканер Retina. Сканер Xspider. Пример использования средств активного аудита. Инструментальные средства анализа рисков. Количественный подход к анализу рисков на примере RiskWatch. Выбор оптимальной стратегии защиты компании.
5		Проблемы развития теории и практики обеспечения информационной безопасности. Основные понятия и определения в области информационной безопасности. Термины, определяющие научную основу информационной безопасности. Термины, определяющие предметную основу информационной безопасности. Термины, определяющие характер деятельности по обеспечению информационной безопасности. Определение информационной безопасности в свете информационных проблем современного общества. Основные составляющие информационной безопасности. Значение информационной безопасности для субъектов информационных отношений. Составляющие национальных интересов Российской Федерации в информационной сфере. Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Международное сотрудничество в области информационной безопасности: проблемы и перспективы.
6		Основные цели и задачи аудита безопасности и анализа рисков. Актуальность аудита безопасности и анализа рисков. Оценка уровня безопасности компьютерных информационных систем. Возможные виды аудита безопасности компьютерных информационных систем. Возможные методики аудита безопасности компьютерных информационных систем. Возможные алгоритмы аудита безопасности компьютерных

№ п/п	Наименование разделов и тем	Содержание
		информационных систем. Анализ информационных рисков. Методы оценивания информационных рисков. Роль анализа рисков в процессе создания корпоративной системы информационной безопасности (на примере модели LifeCycle Security). Возможная методика реорганизации корпоративной системы безопасности. Проектирование системы обеспечения безопасности объекта. Аналитический обзор инструментальных средств для анализа рисков и защищенности корпоративных систем Intranet/Internet. Инструментальные проверки уровня безопасности. Internet Scanner и System Security Scanner. Сканер уязвимости Symantec NetRecon. Система централизованного управления безопасностью Enterprise Security Manager. Сканер уязвимости системы безопасности Cisco Secure Scanner (NetSonar). Сканер Retina. Сканер Xspider. Пример использования средств активного аудита. Инструментальные средства анализа рисков. Количественный подход к анализу рисков на примере RiskWatch. Выбор оптимальной стратегии защиты компании

5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
1	Развитие информационного общества и информационная безопасность, кибербезопасность. Понятие и сущность защиты информации. Цели защиты информации. Концептуальная модель информационной безопасности. Предмет защиты информации. Информация как объект права собственности. Объект защиты информации. Угрозы информационной безопасности: случайные и преднамеренные. Модель гипотетического нарушителя информационной безопасности. Системное обеспечение защиты информации. Основные принципы построения системы защиты. Методы защиты информации. Построение систем защиты от угроз нарушения конфиденциальности информации. Модель системы защиты. Организационные меры и меры обеспечения физической безопасности.
5	Анализ информационных рисков в финансово-кредитных организациях. Аналитический обзор инструментальных средств для анализа рисков и защищенности корпоративных систем Intranet/Internet. Инструментальные проверки уровня безопасности. Internet Scanner и System Security Scanner. Сканер уязвимости Symantec NetRecon. Система централизованного управления безопасностью Enterprise Security Manager. Сканер уязвимости системы безопасности Cisco Secure Scanner (NetSonar). Сканер Retina. Сканер Xspider. Пример использования средств активного аудита. Инструментальные средства анализа рисков. Количественный подход к анализу рисков на примере RiskWatch. Выбор оптимальной стратегии защиты компании.
2	Общее подходы и мероприятия по защите информации и кибербехопасности в финансово-кредитных организациях Правовое регулирование в сфере защиты информации

№ раздела и темы	Содержание и формы проведения
	Анализ информационных рисков Инструментальные средства анализа информационных рисков. дентификация и аутентификация. Разграничение доступа. Криптографические методы обеспечения конфиденциальности информации. Методы защиты
3	Меры и средства обеспечения свойств информационной кибербезопасности в финансовом секторе. Основные определения. Монитор безопасности обращений. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом. Скрытые каналы передачи информации.
4	нформация как объект преступных посягательств. Система правоохранительных органов РФ, связанных с информационной сферой. Понятие компьютерных преступлений и их классификация. Субъект преступлений в сфере компьютерной информации: особенности. Преступления, совершенные с помощью компьютера и их особенности. Основы расследования компьютерных преступлений. Доказательства и доказывание. Международное право при компьютерных инцидентах. Нормы уголовного права некоторых зарубежных стран. Правовые докуме. нформация как объект преступных посягательств. Система правоохранительных органов РФ, связанных с информационной сферой. Понятие компьютерных преступлений и их классификация. Субъект преступлений в сфере компьютерной информации: особенности. Преступления, совершенные с помощью компьютера и их особенности. Основы расследования компьютерных преступлений. Доказательства и доказывание. Международное право при компьютерных инцидентах. Нормы уголовного права некоторых зарубежных стран. Правовые документы по информационной безопасности. Технические документы по информационной безопасности.

6. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине (полный текст приведен в приложении к рабочей программе)

6.1. Текущий контроль

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
1	1. Развитие информационного общества и информационная безопасность, кибербезопасност	ПК-5	З.Знать основные направления анализа информации бухгалтерской (финансовой) отчетности	1	10тестов по 2 балла за вопрос (20)

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
	ь		У.Уметь рассчитывать основные показатели финансового состояния по данным бухгалтерской (финансовой) отчетности организаций, ведомств, предприятий различных форм собственности и интерпретировать полученные результаты Н.Владеть навыком принятия управленческих решений на основе анализа информации, содержащейся в бухгалтерской (финансовой) отчетности		
2		ПК-5	З.Знать основные направления анализа информации бухгалтерской (финансовой) отчетности У.Уметь рассчитывать основные показатели финансового состояния по данным бухгалтерской (финансовой) отчетности организаций, ведомств, предприятий различных форм собственности и интерпретировать полученные результаты Н.Владеть навыком принятия управленческих решений на основе анализа информации, содержащейся в бухгалтерской	2	каждое выбранное задание (2 выбрать) оценивается в 15 баллов (30)

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			(финансовой) отчетности		
3	3. Меры и средства обеспечения свойств информационной кибербезопасности в финансовом секторе	ПК-10	З.Знать основные принципы использования современных технических средств и информационных технологий, используемых для целей коммуникации У.Уметь осуществлять коммуникации с использованием современных технических средств и информационных технологий Н.Владеть навыком решения коммуникатиных задач посредством технических средств с использованием информационных технологий	3	выполненое тестовое задание 2 балла за вопрос (20)
4	5. Анализ информационных рисков в финансово-кредитных организациях	ПК-5	З.Знать основные направления анализа информации бухгалтерской (финансовой) отчетности У.Уметь рассчитывать основные показатели финансового состояния по данным бухгалтерской (финансовой) отчетности организаций, ведомств, предприятий различных форм собственности и интерпретировать полученные результаты Н.Владеть навыком принятия управленческих решений на основе анализа информации,	4	2 задания по 15 баллов каждое (30)

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			содержащейся в бухгалтерской (финансовой) отчетности		
				Итого	**100**

6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Экзамен в семестре 42.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

1-й вопрос билета (40 баллов), вид вопроса: Тест/проверка знаний. Критерий: 2 балла за вопрос.

Компетенция: ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии
Знание: Знать основные принципы использования современных технических средств и информационных технологий, используемых для целей коммуникации
1. 1. Спам распространяющий поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей — это:
2. 3. Агрессивное потребление ресурсов является угрозой:
3. 5. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
4. 6. Что не относится к непреднамеренным воздействиям?
5. 8. Какие принципы кибербезопасности используютсяв Федеральном казначействе
6. 9. Какам образом Банк Росссии обеспечивает защиту своей безопасности
Компетенция: ПК-5 способность анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в отчетности предприятий различных форм собственности, организаций, ведомств и т. д. и использовать полученные сведения для принятия управленческих решений
Знание: Знать основные направления анализа информации бухгалтерской (финансовой) отчетности
7. 10. Кибербезопасность это
8. 2. Доступность достигается за счет применения мер, направленных на повышение:
9. 4. Захват ресурсов с помощью хакерских программ, бомбардировка запросами сервера и т.п. типы атак относятся к виду:
10. 7. Что может указывать на изменение сообщения?

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УМЕНИЙ:

2-й вопрос билета (30 баллов), вид вопроса: Задание на умение. Критерий: выполненное задание 30 баллов.

Компетенция: ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии
Умение: Уметь осуществлять коммуникации с использованием современных технических средств и информационных технологий
Задача № 1. принять решение с использованием информационных технологий
Компетенция: ПК-5 способность анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в отчетности предприятий различных форм собственности, организаций, ведомств и т. д. и использовать полученные сведения для принятия управленческих решений
Умение: Уметь рассчитывать основные показатели финансового состояния по данным бухгалтерской (финансовой) отчетности организаций, ведомств, предприятий различных форм собственности и интерпретировать полученные результаты
Задача № 2. проанализировать представленную информацию

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ:

3-й вопрос билета (30 баллов), вид вопроса: Задание на навыки. Критерий: 30 баллов за задание.

Компетенция: ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии
Навык: Владеть навыком решения коммуникатиных задач посредством технических средств с использованием информационных технологий
Задание № 1. решить поставленную задачу используя технические средства и информационные технологии
Компетенция: ПК-5 способность анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в отчетности предприятий различных форм собственности, организаций, ведомств и т. д. и использовать полученные сведения для принятия управленческих решений
Навык: Владеть навыком принятия управленческих решений на основе анализа информации, содержащейся в бухгалтерской (финансовой) отчетности
Задание № 2. для принятия управленческих решений оценить данные

ОБРАЗЕЦ БИЛЕТА

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение
высшего образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «БГУ»)

Направление - 38.03.01 Экономика
Профиль - Финансы и кредит, бухгалтерский учет и налогообложение
Кафедра финансов и финансовых институтов
Дисциплина - Кибербезопасность финансово-кредитных организаций

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Тест (40 баллов).
2. принять решение с использованием информационных технологий (30 баллов).
3. для принятия управленческих решений оценить данные (30 баллов).

Составитель _____ М.Г. Жигас

Заведующий кафедрой _____ Т.В. Щукина

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

а) основная литература:

1. Информационная безопасность в банках. закон и порядок// Банковские технологии
2. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. допущено УМО по образованию в обл. прикладной информатики. учеб. пособие. 3-е изд., перераб. и доп./ Е. К. Баранова, А. В. Бабаш.- М.: ИНФРА-М, 2016.-321 с.
3. Гришина Н. В. Комплексная система защиты информации на предприятии. учеб. пособие для вузов. рек. УМО вузов РФ по образованию в обл. историко-архивоведения/ Н. В. Гришина.- М.: ФОРУМ, 2014.-238 с.
4. Обеспечение информационной безопасности бизнеса. 2-е изд., перераб. и доп./ В. В. Андрианов [и др.].- М.: Альпина Паблишерз, 2011.-371 с.
5. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98349.html (дата обращения: 16.06.2021). — Режим доступа: для авторизир. пользователей
6. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/108023.html (дата обращения: 16.06.2021). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

1. Астахов А. А. Александр Михайлович Искусство управления информационными рисками/ Александр Астахов.- М.: ДМК Пресс, 2010.-306 с.
2. Крупчик А. Правильное построение и внедрение политики безопасности в финансовом учреждении/ А. Крупчик// Номер журнала, № 8, С. 102, 2010, ч.з 2-202
3. Духан Е. И., Корольков Ю. Д., Синадский Н. И. Средства криптографической защиты компьютерной информации. учеб. пособие/ Е. И. Духан, Ю. Д. Корольков, Н. И. Синадский.- Иркутск: Изд-во ИГУ, 2012.-113 с.
4. Безверхая Е.Н.Экономическая безопасность предприятия: сущность и факторы[Электронный ресурс]/ Е.Н.Безверхая, И.И.Губа, К.А.Ковалева // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2015. – вып. № 108/2015. – Режим доступа: http://cyberleninka.ru/article/n/ekonomicheskaya-bezopasnost-predpriyatiya-suschnost-i-faktory

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая профессиональные базы данных и информационно-справочные системы

Для освоения дисциплины обучающемуся необходимы следующие ресурсы информационно-телекоммуникационной сети «Интернет»:

– Сайт Байкальского государственного университета, адрес доступа: http://bgu.ru/, доступ круглосуточный неограниченный из любой точки Интернет

– Журнал "Директор информационной службы", адрес доступа: https://www.osp.ru/cio. доступ неограниченный

– КиберЛенинка, адрес доступа: http://cyberleninka.ru. доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных

публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению
– Официальный сайт Федерального казначейства РФ, адрес доступа: http://roskazna.ru. доступ неограниченный
– Сайт Банка России, адрес доступа: http://www.cbr.ru. доступ неограниченный
– Сайт Всемирного банка, адрес доступа: http://www.worldbank.org/. доступ неограниченный
– Сайт для поиска книг и журналов открытого доступа издательства Elsevier, адрес доступа: http://www.sciencedirect.com/ . доступ неограниченный
– Сайт Министерства финансов РФ, адрес доступа: http://minfin.ru/ru/. доступ неограниченный
– Сайт национального бюро экономических исследований, адрес доступа: http://www.nber.org/. доступ неограниченный
– Учебники онлайн, адрес доступа: http://uchebnik-online.com/. доступ неограниченный

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

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании. Для успешного освоения курса обучающиеся должны иметь первоначальные знания в области информатики, финансов, страхования, банкоского дела, Банка России.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций студенту необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические (семинарские) занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое (семинарское) занятие сообщается обучающимся до его проведения. На семинаре преподаватель организует обсуждение этой темы, выступая в качестве организатора, консультанта и эксперта учебно-познавательной деятельности обучающегося.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы студентов с участием преподавателей являются:

• текущие консультации;

• коллоквиум как форма контроля освоения теоретического содержания дисциплин: (в часы консультаций, предусмотренные учебным планом);

• прием и разбор домашних заданий (в часы практических занятий);

• прием и защита лабораторных работ (во время проведения занятий);

• выполнение курсовых работ в рамках дисциплин (руководство, консультирование и защита курсовых работ в часы, предусмотренные учебным планом) и др.

Основными видами самостоятельной работы студентов без участия преподавателей являются:

• формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

• самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;

• написание рефератов, докладов;

• подготовка к семинарам и лабораторным работам;

• выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

В учебном процессе используется следующее программное обеспечение:

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

В учебном процессе используется следующее оборудование: