МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Набережночелнинский институт (филиал)
Экономическое отделение

Утверждаю

Первый заместитель директора
НЧИ КФУ Симонова Л. А.

"__" _____ 20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Информационная безопасность Б1.В.ОД.8

Специальность: 38.05.01 - Экономическая безопасность
Специализация: Экономико-правовое обеспечение экономической безопасности
Квалификация выпускника: экономист
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2019
Автор(ы): Гареева Г.А.
Рецензент(ы): Макаров А.Н.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Махмутов И. И.
Протокол заседания кафедры No ___ от "____" _____ 20__г.
Учебно-методическая комиссия Высшей школы экономики и права (Экономическое отделение) (Набережночелнинский институт (филиал)):
Протокол заседания УМК No ____ от "____" _____ 20__г.

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Гареева Г.А. (Кафедра экономики предприятий и организаций, Экономическое отделение), GAGareeva@kpfu.ru

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

Выпускник, освоивший дисциплину, должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-12	Способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, систематизации, обработки и передачи информации
ПК-11	Способностью реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать и использовать в интересах выявления рисков и угроз экономической безопасности, предупреждения, пресечения, раскрытия и расследования преступлений и иных правонарушений в сфере экономики
ПК-20	Способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности
ПК-44	Способностью осуществлять документационное обеспечение управленческой деятельности

Выпускник, освоивший дисциплину:

Должен знать:

- - основы администрирования вычислительных сетей;
- - возможные уязвимости угрозы воздействия нарушителей;
- - методы и программно-аппаратные средства ограничения доступа;
- - методы и программно-аппаратные средства защиты от изучения и внешних воздей-ствий.

Должен уметь:

- - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
- - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- - анализировать и оценивать угрозы информационной безопасности объекта;
- - анализировать возможные уязвимости в конкретных информационно- телекоммуникационных системах.

Должен владеть:

- - навыками выявления и уничтожения компьютерных вирусов;
- - методами и средствами выявления угроз безопасности автоматизированным системам;
- - навыками определения наиболее опасных уязвимостей и угроз;
- - навыками применения штатных средств защиты информации.

Должен демонстрировать способность и готовность:

-применять полученные знания на практике

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Данная учебная дисциплина включена в раздел "Б1.В.ОД.8 Дисциплины (модули)" основной профессиональной образовательной программы 38.05.01 "Экономическая безопасность (Экономико-правовое обеспечение экономической безопасности)" и относится к обязательным дисциплинам.
Осваивается на 4 курсе в 8 семестре.

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

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 32 часа(ов), в том числе лекции - 16 часа(ов), практические занятия - 16 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 40 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 8 семестре.

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

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Основы информационной безопасности.	8	1	1	0	4
2.	Тема 2. Основные определения и критерии классификации угроз	8	1	1	0	4
3.	Тема 3. Стандарты и спецификации в области информационной безопасности	8	2	2	0	4
4.	Тема 4. Основные принципы криптографической зашиты информации	8	2	2	0	4
5.	Тема 5. Вредоностные программы и компьютерные вирусы	8	1	1	0	4
6.	Тема 6. Типовые удаленные атаки в глобальных компьютерных сетях	8	2	2	0	4
7.	Тема 7. Механизмы реализации удаленных атак в глобальной сети INTERNET	8	2	2	0	4
8.	Тема 8. Средства управления безопасностью в архитектуре операционных систем WINDOWS	8	2	2	0	4
9.	Тема 9. Безопасность программного обеспечения	8	3	3	0	8
	Итого		16	16	0	40

4.2 Содержание дисциплины

Тема 1. Основы информационной безопасности.

Понятие информационной безопасности.

Основные составляющие информационной безопасности.

Важность и сложность проблемы информационной безопасности.

Сценарии реализации угроз информационной безопасности.

Тема 2. Основные определения и критерии классификации угроз

Основные понятия об угрозах. Наиболее распространенные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.

Законодательный уровень информационной безопасности.

Понятие о законодательном уровне информационной безопасности. Обзор российского законодательства в области информационной безопасности. Обзор зарубежного законодательства в области информационной безопасности. О текущем состоянии российского законодательства в области информационной безопасности

Тема 3. Стандарты и спецификации в области информационной безопасности

Оценочные стандарты и технические спецификации.

"Оранжевая книга" как оценочный стандарт.

Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 ?Общие критерии оценки безопасности информационных технологий?.

Тема 4. Основные принципы криптографической зашиты информации

Понятие криптографии.

Понятия о симметричных и асимметричных криптосистемах.

Понятие криптоанализа.

Аппаратно-программные криптографические средства защиты информации

Тема 5. Вредоностные программы и компьютерные вирусы

Основные понятия. Способы распространения вредоносных программ. Операционная система. Уязвимости и заплаты. Последствия заражений вредоносной программой. Классификация вредоносных программ. Примеры угроз безопасности информации реализуемых вредоносными программами. История компьютерных вирусов. Ответственность за написание и распространение вредоносных программ.

Тема 6. Типовые удаленные атаки в глобальных компьютерных сетях

Понятие типовой удаленной атаки.

Классификация удаленных атак.

Типовые удаленные атаки и механизмы их реализации.

Анализ типовых уязвимостей позволяющих реализовать успешные удаленные атаки.

Тема 7. Механизмы реализации удаленных атак в глобальной сети INTERNET

Анализ сетевого трафика. Ложный ARP-сервер. Ложный DNS-сервер. Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети Internet ложного маршрутизатора. Подмена одного из субъектов TCP-соединения в сети Internet. Нарушение работоспособности хоста в сети Internet при использовании направленного ?шторма? ложных TCP-запросов на создание соединения, либо при переполнении очереди запросов

Тема 8. Средства управления безопасностью в архитектуре операционных систем WINDOWS

Система безопасности.

Средства управления безопасностью.

Основные компоненты системы безопасности.

Средства управления безопасностью в архитектуре операционных систем WINDOWS

Тема 9. Безопасность программного обеспечения

Введение в защиту ПО. Угрозы безопасности ПО. Разрушающие программные средства. Модель угроз и принципы обеспечения безопасности ПО. Элементы модели угроз эксплуатационной безопасности ПО. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла. Методы и средства анализа безопасности ПО.

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

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301).

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Положение от 24 декабря 2015 г. № 0.1.1.67-06/265/15 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Положение № 0.1.1.67-06/241/15 от 14 декабря 2015 г. "О формировании фонда оценочных средств для проведения текущей, промежуточной и итоговой аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Положение № 0.1.1.56-06/54/11 от 26 октября 2011 г. "Об электронных образовательных ресурсах федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет""

Регламент № 0.1.1.67-06/66/16 от 30 марта 2016 г. "Разработки, регистрации, подготовки к использованию в учебном процессе и удаления электронных образовательных ресурсов в системе электронного обучения федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Регламент № 0.1.1.67-06/11/16 от 25 января 2016 г. "О балльно-рейтинговой системе оценки знаний обучающихся в федеральном государственном автономном образовательном учреждении высшего образования "Казанский (Приволжский) федеральный университет""

Регламент № 0.1.1.67-06/91/13 от 21 июня 2013 г. "О порядке разработки и выпуска учебных изданий в федеральном государственном автономном образовательном учреждении высшего профессионального образования "Казанский (Приволжский) федеральный университет""

6. Фонд оценочных средств по дисциплине (модулю)

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
Семестр 8			
	Текущий контроль		
1	Письменная работа	ПК-20 , ОК-12	1. Основы информационной безопасности. 2. Основные определения и критерии классификации угроз 4. Основные принципы криптографической зашиты информации 8. Средства управления безопасностью в архитектуре операционных систем WINDOWS
2	Контрольная работа	ОК-12	8. Средства управления безопасностью в архитектуре операционных систем WINDOWS
3	Дискуссия	ОК-12	1. Основы информационной безопасности. 2. Основные определения и критерии классификации угроз 3. Стандарты и спецификации в области информационной безопасности 4. Основные принципы криптографической зашиты информации 5. Вредоносные программы и компьютерные вирусы
	Зачет		

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Семестр 8					
Текущий контроль					
Письменная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.	1

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Контрольная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.	2
Дискуссия	Высокий уровень владения материалом по теме дискуссии. Превосходное умение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения. Высокий уровень этики ведения дискуссии.	Средний уровень владения материалом по теме дискуссии. Хорошее умение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения. Средний уровень этики ведения дискуссии.	Низкий уровень владения материалом по теме дискуссии. Слабое умение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения. Низкий уровень этики ведения дискуссии.	Недостаточный уровень владения материалом по теме дискуссии. Неумение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения. Отсутствие этики ведения дискуссии.	3
	Зачтено		**Не зачтено**		
Зачет	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных программой дисциплины.		Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.		

6.3 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

Семестр 8

Текущий контроль

1. Письменная работа

Темы 1, 2, 4, 8

Занятие 1.

Задания для самостоятельной работы студентов: изучить теоретические и практические материалы по теме: ?Цели и задачи обеспечения информационной безопасности? по рекомендуемой литературе.

Занятие 2.

Задание для практической работы: Анализ угроз информационной безопасности для малого предприятия и построение модели системы защиты информации.

Задания для самостоятельной работы студентов: изучить теоретические и практические материалы по теме: ?Архитектура СЗИ организации и основные требования к средствам защиты? по рекомендуемой литературе.

Занятие 3.

Задания для самостоятельной работы студентов: изучить теоретические и практические материалы по теме: "Анализ и управление рисками в сфере информационной безопасности" по рекомендуемой литературе.

Занятие 4.

Задания для самостоятельной работы студентов: изучить теоретические и практические материалы по теме: "Криптографическая защита информации" по рекомендуемой литературе.

Занятие 5.

Задание для письменной работы студентов:

1. Методы защиты информации при передаче в телекоммуникационных сетях.
2. Вредоносное программное обеспечение и методы борьбы с ним.
3. Модель угроз и принципы обеспечения безопасности ПО.
4. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла.
5. Методы и средства анализа безопасности ПО.

2. Контрольная работа

Тема 8

Средства обеспечения безопасности ОС Windows

Цель: изучить модель безопасности операционной системы Windows

1.Понятия: информация, информатизация, информационные технологии, информационные ресурсы.

2.Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.

3.Элементарные модели СЗИ организации. Семирубежная модель защиты.

4.Содержание процесса эксплуатации СЗИ организации.

5.Анализ информационных рисков, угроз и уязвимостей системы.

6.Особенности защиты мультимедийного контента в телекоммуникационных сетях.

7.Классификация и основные особенности различных видов вредоносных программ.

8.Возможности и особенности сетевых вредоносных программ.

9.Виды нарушений работоспособности удаленного компьютера со стороны вредоносных программ.

10.Современное антивирусное программное обеспечение.

3. Дискуссия

Темы 1, 2, 3, 4, 5

Занятие 1.

Понятия : информация, информационная безопасность. Цели и задачи обеспечения информационной безопасности. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.

Вопросы для обсуждения:

1. Понятия: информация, информатизация, информационные технологии, информацион-ные ресурсы.
2. Место информационной безопасности в национальной безопасности РФ.
3. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.
4. Виды и источники угроз информационной безопасности РФ.
5. Структура государственной системы обеспечения информационной безопасности РФ.
6. Правовое регулирование информационной сферы в РФ.
7. Основные нормативно-методические материалы.

Занятие 2.

Вопросы для обсуждения:

1. Функциональное построение СЗИ организации и назначение основных подразделений.
2. Элементарные модели СЗИ организации. Семирубежная модель защиты.
3. Последовательность и содержание основных этапов проектирования СЗИ организации.
4. Содержание процесса эксплуатации СЗИ организации.

Занятие 3.

Вопросы для обсуждения:

1. Анализ информационных рисков, угроз и уязвимостей системы.
2. Оценка рисков по двум факторам.
3. Анализ информационных рисков, угроз и уязвимостей системы.
4. Оценка рисков по трем факторам.

Занятие 4.

Криптографическая защита информации.

Вопросы для обсуждения:

1. Отечественный стандарт симметричного шифрования ГОСТ 28147-89.
2. Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП.
3. Отечественный стандарт цифровой подписи ГОСТ Р34.10-2012.
4. Защищенный электронный документооборот.
5. Особенности защиты мультимедийного контента в телекоммуникационных сетях.

Занятие 5.

Методы защиты информации при передаче в телекоммуникационных сетях. Вредоносное программное обеспечение и методы борьбы с ним.

Вопросы для обсуждения:

1. Вредоносный программный код документов офисных приложений и его возможности.
2. Классификация и основные особенности различных видов вредоносных программ.
3. Возможности и особенности сетевых вредоносных программ.
4. Виды несанкционированного копирования компьютерной информации.
5. Виды нарушений работоспособности удаленного компьютера со стороны вредоносных программ.
6. Современное антивирусное программное обеспечение.

Зачет

Вопросы к зачету:
1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Важность и сложность проблемы информационной безопасности.
4. Сценарии реализации угроз информационной безопасности.
5. Основные понятия об угрозах.
6. Наиболее распространенные угрозы доступности.
7. Основные угрозы целостности.
8. Основные угрозы конфиденциальности.
9. Понятие о законодательном уровне информационной безопасности.
10. Обзор российского законодательства в области информационной безопасности.
11. Обзор зарубежного законодательства в области информационной безопасности.
12. О текущем состоянии российского законодательства в области информационной без-опасности
13. Оценочные стандарты и технические спецификации.
14. ?Оранжевая книга? как оценочный стандарт.
15. Информационная безопасность распределенных систем.
16. Рекомендации X.800.
17. Стандарт ISO/IEC 15408 ?Общие критерии оценки безопасности информационных тех-нологий?.
18. Понятие криптографии.
19. Понятия о симметричных и асимметричных криптосистемах.
20. Понятие криптоанализа.
21. Аппаратно-программные криптографические средства защиты информации
22. Вредоностные программы и компьютерные вирусы. Основные понятия.
23. Способы распространения вредоносных программ.
24. Операционная система. Уязвимости и заплаты.
25. Последствия заражений вредоносной программой.
26. Классификация вредоностных программ.
27. Примеры угроз безопасности информации реализуемых вредоностными программами.
28. История компьютерных вирусов.
29. Ответственность за написание и распространение вредоносных программ.
30. Понятие типовой удаленной атаки.
31. Классификация удаленных атак.
32. Типовые удаленные атаки и механизмы их реализации.
33. Анализ типовых уязвимостей, позволяющих реализовать успешные удаленные атаки.
34. Механизмы реализации удаленных атак в глобальной сети INTERNET.
35. Анализ сетевого трафика.
36. Ложный ARP-сервер.
37. Ложный DNS-сервер.
38. Навязывание хосту ложного маршрута с использованием протокола ICMP с целью со-здания в сети Internet ложного маршрутизатора.
39. Подмена одного из субъектов TCP-соединения в сети Internet.
40. Нарушение работоспособности хоста в сети Internet при использовании направленного ?шторма? ложных TCP-запросов на создание соединения, либо при переполнении очереди запро-сов
41. Средства управления безопасностью в архитектуре операционных систем WINDOWS.
42. Введение в защиту ПО.
43. Угрозы безопасности ПО.
44. Разрушающие программные средства.
45. Модель угроз и принципы обеспечения безопасности ПО.
46. Элементы модели угроз эксплуатационной безопасности ПО.
47. Основные принципы обеспечения безопасности ПО на различных стадиях его жизнен-ного цикла.
48. Методы и средства анализа безопасности ПО.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В КФУ действует балльно-рейтинговая система оценки знаний обучающихся. Суммарно по дисциплине (модулю) можно получить максимум 100 баллов за семестр, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов.

Для зачёта:

56 баллов и более - "зачтено".

55 баллов и менее - "не зачтено".

Для экзамена:

86 баллов и более - "отлично".

71-85 баллов - "хорошо".

56-70 баллов - "удовлетворительно".

55 баллов и менее - "неудовлетворительно".

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Семестр 8			
Текущий контроль			
Письменная работа	Обучающиеся получают задание по освещению определённых теоретических вопросов или решению задач. Работа выполняется письменно и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	1	28
Контрольная работа	Контрольная работа проводится в часы аудиторной работы. Обучающиеся получают задания для проверки усвоения пройденного материала. Работа выполняется в письменном виде и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	2	14
Дискуссия	На занятии преподаватель формулирует проблему, не имеющую однозначного решения. Обучающиеся предлагают решения, формулируют свою позицию, задают друг другу вопросы, выдвигают аргументы и контраргументы в режиме дискуссии. Оцениваются владение материалом, способность генерировать свои идеи и давать обоснованную оценку чужим идеям, задавать вопросы и отвечать на вопросы, работать в группе, придерживаться этики ведения дискуссии.	3	8
Зачет	Зачёт нацелен на комплексную проверку освоения дисциплины. Обучающийся получает вопрос (вопросы) либо задание (задания) и время на подготовку. Зачёт проводится в устной, письменной или компьютерной форме. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

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

7.1 Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Режим доступа: http://znanium.com/catalog/product/405000.

2. Бирюков, А. А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Режим доступа: http://znanium.com/catalog/product/1028060

3. Информационные системы в экономике [Электронный ресурс]: Учебник / Балдин К.В., Уткин В.Б., - 7-е изд. - М.:Дашков и К, 2017. - 395 с.: 60x84 1/16 ISBN 978-5-394-01449-9 - Режим доступа: http://znanium.com/catalog/product/327836

7.2. Дополнительная литература:

1. Баранова Е. К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е.К. Баранова, А.В.Бабаш. - 4-е изд., перераб. и доп. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. - ISBN 978-5-369-01761-6.- Режим доступа: http://znanium.com/catalog/product/957144

2. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. - М. : ИНФРА-М, 2019. - 118 с. + Доп. материалы [Электронный ресурс]. - www.dx.doi.org/10.12737/13571. - Режим доступа: http://znanium.com/catalog/product/991792

3. Информационная безопасность [Электронный ресурс]: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1 - Режим доступа: http://znanium.com/catalog/product/997105

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей - http://znanium.com/bookread.php?book=335362

2. Башлы П. Н. Информационная безопасность и защита информации - http://znanium.com/bookread.php?book=405000

3. Баранова Е. К. Информационная безопасность и защита информации - http://www.bibliorossica.com/book.html?currBookId=6182

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

Вид работ	Методические рекомендации
лекции	В ходе лекционных занятий вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. В ходе подготовки к лабораторным работам изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. При этом учесть рекомендации преподавателя и требования учебной программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой. Подготовить тезисы для выступлений по всем учебным вопросам, выносимым на лабораторную работу. Продумать примеры с целью обеспечения тесной связи изучаемой теории с реальной жизнью. Своевременное и качественное выполнение самостоятельной работы базируется на соблюдении настоящих рекомендаций и изучении рекомендованной литературы. Студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании курсовых и дипломных работ.
практические занятия	Предназначены для оказания помощи студентам по выполнению практических работ в объеме определенного курса или его раздела. Обучающийся 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 преподавателя на практических занятиях; 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 точек зрения различных авторов по затрагиваемым в учебном курсе проблемам; выявление неточностей и некорректного изложения материала в периодической и специальной литературе; 5) периодическое ознакомление с последними теоретическими и практическими достижениями в изучаемой области; 6) проведение собственных научных и практических исследований по одной или нескольким актуальным проблемам; 7) подготовка научных статей для опубликования в периодической печати, выступление на научно-практических конференциях, участие в работе студенческих научных обществ, круглых столах и диспутах.

Вид работ	Методические рекомендации
самостоятельная работа	Подготовка к самостоятельной работе включает 2 этапа: 1й - организационный; 2й - закрепление и углубление теоретических знаний. На первом этапе студент планирует свою самостоятельную работу, которая включает: - уяснение задания на самостоятельную работу; - подбор рекомендованной литературы; - составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку студента к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.
письменная работа	Письменные работы и задания могут быть индивидуальными (по вариантам) и общими. Первоначально студенту необходимо определить цель написания работы по закреплённой теме, а также перечень решаемых вопросов. Относительно оглавления письменной работы следует отметить, что она может носить рабочий, простой или развёрнутый характер. Рабочий (план) представляет собой краткий перечень основных вопросов, решаемых в ходе выполнения работы.
контрольная работа	Подготовку контрольной работы следует начинать с повторения соответствующего раздела учебника, учебных пособий по данной теме и конспектов лекций прочитанных ранее. Контрольная работа излагается логически последовательно, грамотно и разборчиво. Каждая работа обязательно должна иметь титульный лист. При защите студент должен быть готов ответить на вопросы по всем теоретическим положениям работы.
дискуссия	На обсуждение студентов выносятся темы, имеющие проблемный характер. Студентам предлагается на выбор несколько вариантов проблем, связанных с конкретной учебной темой. Тема разбивается на отдельные вопросы, указывается литература, справочные материалы, необходимые для подготовки к дискуссии.
зачет	Изучение дисциплины завершается зачетом. Подготовка к зачету способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к зачету, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На зачете студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине. За 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед зачетом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно. Требования к организации подготовки к зачетам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. При подготовке к зачетам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов. Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

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

Освоение дисциплины "Информационная безопасность" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows Professional 7 Russian

Пакет офисного программного обеспечения Microsoft Office 2010 Professional Plus Russian

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе " БиблиоРоссика", доступ к которой предоставлен обучающимся. В ЭБС " БиблиоРоссика " представлены коллекции актуальной научной и учебной литературы по гуманитарным наукам, включающие в себя публикации ведущих российских издательств гуманитарной литературы, издания на английском языке ведущих американских и европейских издательств, а также редкие и малотиражные издания российских региональных вузов. ЭБС "БиблиоРоссика" обеспечивает широкий законный доступ к необходимым для образовательного процесса изданиям с использованием инновационных технологий и соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

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

Освоение дисциплины "Информационная безопасность" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по специальности: 38.05.01 "Экономическая безопасность" и специализации Экономико-правовое обеспечение экономической безопасности .