МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (КБГУ)

ИНСТИТУТ ПРАВА, ЭКОНОМИКИ И ФИНАНСОВ

КАФЕДРА БУХГАЛТЕРСКОГО УЧЕТА, АНАЛИЗА И АУДИТА

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Руководитель научной программы	**Директор института**
_____А.Х. Шидов	_____М.Х. Гукепшоков
«__»_____20__ г.	«__»_____20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ»

Направление подготовки (специальность)
38.03.01 ЭКОНОМИКА
(код и наименование направления подготовки)

Профиль подготовки
«Информационно-аналитическое и правовое обеспечение экономической безопасности бизнеса»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная

Нальчик 2018

Рабочая программа дисциплины (модуля) «Информационная безопасность экономической деятельности» /сост. Б.В. Казиева – *Нальчик: КБГУ,* 2018. – 41 с.

Рабочая программа предназначена для студентов очной формы обучения по направлению подготовки 38.03.01 Экономика профиль «Информационно-аналитическое и правовое обеспечение экономической безопасности бизнеса» VI семестра, 3 курса.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 38.03.01 Экономика (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 12 ноября 2015 г. №1327 (зарегистрировано в Минюсте России 30 ноября 2015 г. № 39906).

С О Д Е Р Ж А Н И Е

1. Цели и задачи освоения дисциплины (модуля)

Целью освоения дисциплины «Информационная безопасность экономической деятельности» является овладение теоретическими знаниями и формирование практических навыков по диагностике и обеспечению информационной безопасности экономической деятельности предприятий.

Задачами освоения дисциплины «Информационная безопасность экономической деятельности» являются:

– освоить сущность базовых категорий информационной безопасности предприятия;

– ознакомить с нормативно-правовой базой, регулирующей вопросы обеспечения информационной безопасности экономической и финансовой деятельности субъектов хозяйствования;

– передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;

– сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина «Информационная безопасность экономической деятельности» относится к модулю «Дисциплины по выбору» вариативной части Блока 1 «Дисциплины (модули)» основной образовательной программы по направлению подготовки 38.03.01 Экономика, профиль «Информационно-аналитическое и правовое обеспечение экономической безопасности бизнеса».

Для освоения дисциплины слушатели используют знания и практические навыки, сформированные в ходе изучения следующих дисциплин: «Экономическая информатика», «Справочно-информационные системы в экономике», «Статистика», «Бухгалтерский учет и анализ». Успешное освоение данной дисциплины возможно только при комплексном изучении указанных областей знаний, а также при активной самостоятельной работе студентов с законодательными актами, нормативно-справочной, научной, учебной и периодической литературой по изучаемым вопросам дисциплины.

Освоение дисциплины «Информационная безопасность экономической деятельности» необходимо для дальнейшего изучения таких дисциплин и практик, как «Коммерческая тайна и методы защиты конфиденциальной информации», «Организация внутреннего контроля и собственной безопасности бизнеса».

3. Требования к результатам освоения дисциплины (модуля)

В совокупности с другими дисциплинами профиля «Информационно-аналитическое и правовое обеспечение экономической безопасности бизнеса» дисциплина «Информационная безопасность экономической деятельности» направлена на формирование следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по направлению подготовки 38.03.01 – Экономика (уровень бакалавриата):

Профессиональных компетенций (ПК) по видам профессиональной деятельности:

аналитическая, научно-исследовательская деятельность:

ПК-7 – способность, используя отечественные и зарубежные источники информации, собрать необходимые данные, проанализировать их и подготовить информационный обзор и/или аналитический отчет.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

– основные понятия, угрозы и нормативно-правовую базу в области информационной безопасности деятельности предприятия;
– технологии обеспечения безопасности данных предприятия и защиты от вредоносных программ и спама;
– принципы многоуровневой защиты корпоративной информации и управления средствами обеспечения информационной безопасности организации.

УМЕТЬ:

– осуществлять поиск, классификацию и первичную обработку информации для целей обеспечения информационной безопасности деятельности предприятия;
– применять методы подготовки информационных и аналитических отчетов;
– готовить презентации по результатам подготовленного информационного или аналитического материала.

ВЛАДЕТЬ:

– способами обработки, систематизации, оценки и интерпретации информации для целей обеспечения информационной безопасности деятельности предприятия;
– современными методами оценки информации в сфере информационных технологий и защиты информации;
– навыками публичной презентации информационно-аналитических материалов и полемики по ним.

4. Содержание и структура дисциплины (модуля)

Таблица 1. Содержание дисциплины (модуля) «Информационная безопасность экономической деятельности»

№ п/п	Наименование раздела/ темы	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Теоретические основы информационной безопасности предприятия	Основные понятия информационной безопасности. Взаимодействие основных субъектов и объектов обеспечения информационной безопасности. Основные понятия защиты информации. Меры и средства обеспечения информационной безопасности.	Р, ДЗ
2	Угрозы информационной безопасности экономических субъектов	Анализ и классификация угроз информационной безопасности. Анализ угроз в компьютерных сетях. Угрозы безопасности и уязвимости в беспроводных сетях. Криминализация атак на информационные системы. Появление кибероружия для ведения кибервойн.	Р, ДЗ
3	Нормативно-правовые основы информационной безопасности и защиты информации предприятия	Нормативные акты, регулирующие сферу информационной безопасности в РФ. Федеральный закон «Об информации, информационных технологиях и о защите информации». Федеральный закон «О коммерческой тайне». Федеральный закон «О персональных данных». Ответственность за нарушения в сфере компьютерной информации.	Р, ДЗ, Т, К
4	Политика информационной безопасности предприятия	Основные понятия политики информационной безопасности. Структура политики информационной безопасности организации. Базовая и специализированная политики информационной безопасности предприятия. Процедуры обеспечения информационной	Р, ДЗ

		безопасности предприятия. Разработка политики информационной безопасности предприятия. Компоненты архитектуры безопасности корпоративной сети.	
5	Принципы многоуровневой защиты корпоративной информации	Корпоративная система с традиционной структурой. Системы облачных вычислений. Многоуровневый подход к обеспечению информационной безопасности корпоративной информационной системы. Подсистемы информационной безопасности традиционных корпоративных информационных систем.	Р, ДЗ
6	Технологии безопасности данных предприятия	Основные понятия криптографической защиты информации. Электронная цифровая подпись. Инфраструктура управления открытыми ключами PKI. Аутентификация, авторизация и администрирование действий пользователей. Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей VNP.	Р, ДЗ, Т, К
7	Защита от вредоносных программ и спама	Классификация вредоносных программ. Основы работы антивирусных программ. Режимы работы антивирусных программ. Облачная антивирусная технология. Защита персональных компьютеров и корпоративных систем от действия вредоносных программ и вирусов.	Р, ДЗ
8	Управление средствами обеспечения информационной безопасности	Задачи управления информационной безопасностью. Концепция глобального управления безопаснотью GSM. Функционирование системы управления информационной безопасностью корпоративной информационной системы. Аудит безопасности корпоративной информационной системы. Мониторинг безопасности информационной системы компании. Обзор современных систем управления безопасностью корпоративных информационных систем. Обеспечение безопасности облачных технологий.	Р, ДЗ, К, Т, РК

Структура дисциплины (модуля) «Информационная безопасность экономической деятельности»

Таблица 2. Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)

Вид работы	**Трудоемкость, часы**	
	6 семестр	**Всего**
Общая трудоемкость (в часах)	**108**	**108**
Контактная работа (в часах):	**60**	**60**
Лекции (Л)	30	30
Практические занятия (ПЗ)	30	30
Семинарские занятия (СЗ)	*Не предусмотрены*	*Не предусмотрены*
Лабораторные работы (ЛР)	*Не предусмотрены*	*Не предусмотрены*
Самостоятельная работа (в часах):	**21**	**21**
Расчетно-графическое задание (РГЗ)	*Не предусмотрены*	*Не предусмотрены*

Реферат (Р)	7	7
Эссе (Э)	*Не предусмотрены*	*Не предусмотрены*
Контрольная работа (К)	*Не предусмотрены*	*Не предусмотрены*
Самостоятельное изучение разделов/тем	14	14
Курсовой проект (КП), курсовая работа (КР)	*Не предусмотрены*	*Не предусмотрены*
Подготовка и прохождение промежуточной аттестации	27	27
Вид промежуточной аттестации	**экзамен**	**экзамен**

Таблица 3. Лекционные занятия

№ п/п	Тема
1	*Теоретические основы информационной безопасности предприятия. Цели и задачи темы* - изучить основные понятия, объекты и субъекты информационной безопасности, меры и средства ее обеспечения.
2	*Угрозы информационной безопасности экономических субъектов. Цели и задачи темы* - провести анализ и классификацию угроз информационной безопасности, изучить криминализацию атак на информационные системы и появление кибероружия для ведения кибервойн.
3	*Нормативно-правовые основы информационной безопасности и защиты информации предприятия. Цели и задачи темы* – дать характеристику нормативным актам, регулирующим сферу информационной безопасности в РФ.
4	*Политика информационной безопасности предприятия. Цели и задачи темы* - раскрыть основные понятия, структуру политики информационной безопасности, ее процедуры и компоненты архитектуры безопасности корпоративной сети.
5	*Принципы многоуровневой защиты корпоративной информации. Цели и задачи темы* - дать характеристику системам облачных вычислений, раскрыть многоуровневый подход к обеспечению информационной безопасности корпоративной информационной системы.
6	*Технологии безопасности данных предприятия. Цели и задачи темы* - раскрыть основные понятия криптографической защиты информации, изучить процедуры аутентификации, авторизации и администрирования действий пользователей, технологии межсетевого экранирования.
7	*Защита от вредоносных программ и спама. Цели и задачи темы* - привести классификации вредоносных программ, изучить основы работы антивирусных программ, определить процедуры защиты персональных компьютеров и корпоративных систем от действия вредоносных программ и вирусов.
8	*Управление средствами обеспечения информационной безопасности. Цели и задачи темы* - раскрыть задачи управления информационной безопасностью, концепции глобального управления безопаснотью GSM, изучить процедуры аудита и мониторинга безопасности корпоративной информационной системы.

Таблица 4. Практические занятия (Семинарские занятия)

№ п/п	Тема
1	Теоретические основы информационной безопасности предприятия
2	Угрозы информационной безопасности экономических субъектов
3	Нормативно-правовые основы информационной безопасности и защиты информации предприятия
4	Политика информационной безопасности предприятия
5	Принципы многоуровневой защиты корпоративной информации
6	Технологии безопасности данных предприятия
7	Защита от вредоносных программ и спама
8	Управление средствами обеспечения информационной безопасности

Таблица 5. Лабораторные работы – не предусмотрены рабочим планом по направлению 38.03.01 Экономика, профиль «Информационно-аналитическое и правовое обеспечение экономической безопасности бизнеса».

Таблица 6. Самостоятельное изучение разделов дисциплины

№ п/п	Вопросы, выносимые на самостоятельное изучение
1	Криминализация атак на информационные системы
2	Появление кибероружия для ведения кибервойн
3	Федеральный закон «О персональных данных»
4	Ответственность за нарушения в сфере компьютерной информации
5	Разработка политики информационной безопасности предприятия Компоненты архитектуры безопасности корпоративной сети
6	Компоненты архитектуры безопасности корпоративной сети
7	Многоуровневый подход к обеспечению информационной безопасности корпоративной информационной системы
8	Подсистемы информационной безопасности традиционных корпоративных информационных систем
9	Технологии межсетевого экранирования
10	Технологии виртуальных защищенных сетей VNP
11	Облачная антивирусная технология
12	Защита персональных компьютеров и корпоративных систем от действия вредоносных программ и вирусов
13	Обзор современных систем управления безопасностью корпоративных информационных систем
14	Обеспечение безопасности облачных технологий

5. Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации

Конечными результатами освоения программы дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы.

В ходе изучения дисциплины предусматриваются ***текущий, рубежный контроль и промежуточная аттестация.***

5.1. Оценочные материалы для текущего контроля. *Цель текущего контроля* – оценка результатов работы в семестре и обеспечение своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающегося. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине «Информационная безопасность экономической деятельности».

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины «Информационная безопасность экономической деятельности» и включает: выполнение практических работ, самостоятельное выполнение индивидуальных домашних заданий (например, решение задач) с отчетом (защитой) в установленный срок, написание рефератов.

Оценка качества подготовки на основании выполненных заданий ведется преподавателем (с обсуждением результатов), баллы начисляются в зависимости от сложности задания.

5.1.1. Вопросы по темам дисциплины «Информационная безопасность экономической деятельности»

Тема №1. Теоретические основы информационной безопасности предприятия

1. Дайте определение понятия «информационная безопасность».
2. Дайте определение понятия «доступность информации». Поясните, что понимается под доступностью компонента и ресурса.
3. Дайте определение понятия «целостность информации». Поясните, что понимается под целостностью компонента и ресурса.

4. Дайте определение понятия «конфиденциальность информации». Поясните, что понимается под правом и правилом доступа к информации.
5. Дайте определение понятия «объект информатизации».
6. Дайте определение понятия «информационные ресурсы (активы)».
7. Дайте определение понятий «собственник информации», «владелец информации», «пользователь информации».
8. Дайте определение понятия «защита информации».
9. Дайте определение понятия «объект защиты информации».
10. Дайте определение понятия «эффективность защиты информации». Поясните, в чем цель защиты информации.
11. Дайте определение понятий «санкционированный доступ к информации» и «несанкционированный доступ к информации».
12. Дайте определение понятий «идентификация субъекта» и «идентификатор».
13. Дайте определение понятий «аутентификация субъекта» и «авторизация субъекта».
14. Дайте определение понятий «защита информации от разглашения», «защищенная система», «средство защиты информации», «способ защиты информации», «комплекс средств защиты информации».
15. Дайте определение понятий «техника защиты информации» и «система защиты информации».
16. Раскройте суть фрагментарного подхода к решению проблемы обеспечения безопасности компьютерных систем и сетей.
17. Раскройте суть комплексного подхода к решению проблемы обеспечения безопасности компьютерных систем и сетей.
18. Раскройте систему мер защиты интересов субъектов информационных отношений.
19. Перечислите меры защиты информации законодательного уровня.
20. Перечислите меры защиты информации административно-организационного уровня.
21. Перечислите меры защиты информации программно-технического уровня.
22. Раскройте основные рекомендации ISTF по обеспечению информационной безопасности электронного бизнеса.

Тема №2. Угрозы информационной безопасности экономических субъектов

1. Раскройте понятие «угрозы нарушения целостности» информации.
2. Раскройте понятие «угрозы нарушения доступности» информации.
3. Раскройте понятие «угрозы нарушения конфиденциальности» информации.
4. Раскройте классификацию угроз информационной безопасности по природе их возникновения.
5. Раскройте классификацию угроз информационной безопасности по степени преднамеренности их возникновения.
6. Раскройте классификацию угроз информационной безопасности по источнику их возникновения.
7. Раскройте классификацию угроз информационной безопасности по положению источника их возникновения.
8. Раскройте классификацию угроз информационной безопасности по степени их зависимости от активности информационной системы.
9. Раскройте классификацию угроз информационной безопасности по степени их воздействия на информационную систему.
10. Раскройте классификацию угроз информационной безопасности по этапам доступа пользователей или программ к ресурсам информационной системы.
11. Раскройте классификацию угроз информационной безопасности по способу доступа к ресурсам информационной системы.
12. Раскройте классификацию угроз информационной безопасности по текущему месту расположения информации, хранимой и обрабатываемой в информационной системе.

13. Раскройте классификацию угроз на случайные и преднамеренные. Приведите свои примеры каждого типа угроз.
14. Раскройте понятие «гипотетическая модель потенциального нарушителя».
15. Раскройте понятие «инсайдер».
16. Раскройте понятие «несанкционированный доступ».
17. Перечислите основные каналы несанкционированного доступа.
18. Перечислите основные виды несанкционированного доступа.
19. Раскройте содержание такого вида несанкционированного доступа, как «перехват паролей».
20. Раскройте содержание такого вида несанкционированного доступа, как «маскарад».
21. Раскройте содержание такого вида несанкционированного доступа, как «незаконное использование привилегий».
22. Раскройте понятие «компьютерный вирус».
23. Перечислите виды компьютерных вирусов.
24. Раскройте понятие «сетевой червь».
25. Раскройте понятие «троянский конь».
26. Перечислите меры защиты от компьютерных вирусов.
27. Раскройте понятие «спам».
28. Раскройте понятие «сетевая атака».
29. Перечислите основные виды сетевых атак.
30. Раскройте понятие «атака доступа». Раскройте виды атак доступа.
31. Раскройте понятие «атака модификации». Раскройте виды атак модификации.
32. Раскройте понятие «атака отказа в обслуживании». Раскройте виды атак отказа в обслуживании.
33. Раскройте понятие «комбинированная атака». Раскройте виды комбинированных атак.
34. Раскройте понятие «фишинг».
35. Раскройте понятие «применение ботнетов».
36. Опишите основные угрозы безопасности в беспроводных сетях.
37. Опишите суть кибершантажа.
38. Опишите суть кибероружия.

<u>Тема №3.</u> Нормативно-правовые основы информационной безопасности и защиты информации предприятия

1. Раскройте систему нормативно-правовых актов в области информационной безопасности в РФ.
2. Охарактеризуйте предмет правового регулирования в сфере информационной безопасности.
3. Раскройте гарантии в сфере информации и информационной безопасности, закрепленные в нормах Конституции РФ.
4. Раскройте основные задачи обеспечения информационной безопасности, закрепленные в Концепции национальной безопасности РФ.
5. Перечислите подзаконные нормативные акты, регулирующие сферу информационной безопасности.
6. Дайте краткую характеристику ФЗ «Об информации, информационных технологиях и о защите информации».
7. Опишите, что вы понимаете под информацией, предоставляемой по соглашению лиц, участвующих в соответствующих отношениях. Приведите свои примеры такой информации.
8. Опишите, что вы понимаете под информацией, которая в соответствии с федеральными законами подлежит предоставлению или распространению. Приведите свои примеры такой информации.

9. Опишите, что вы понимаете под информацией, распространение которой в РФ ограничивается или запрещается. Приведите свои примеры такой информации.
10. Перечислите задачи защиты информации, определенные в ФЗ «Об информации, информационных технологиях и о защите информации».
11. Дайте краткую характеристику Федеральному закону «О коммерческой тайне».
12. Дайте краткую характеристику Федеральному закону «О персональных данных».
13. Дайте определение понятию «персональные данные».
14. Перечислите основные принципы обработки персональных данных.
15. Дайте определение понятию «коммерческая тайна» и «информация, составляющая коммерческую тайну».
16. Перечислите сведения, которые не могут составлять коммерческую тайну.
17. Охарактеризуйте ответственность за неправомерный доступ к компьютерной информации.
18. Охарактеризуйте ответственность за создание, использование и распространение вредоносных программ для ЭВМ.
19. Охарактеризуйте ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети.

Тема №4. Политика информационной безопасности предприятия

1. Дайте определение понятию «политика информационной безопасности».
2. Перечислите разделы Политики информационной безопасности предприятия.
3. Раскройте содержание раздела «Описание проблемы» Политики информационной безопасности предприятия.
4. Раскройте содержание раздела «Область применения» Политики информационной безопасности предприятия.
5. Раскройте содержание раздела «Позиция организации» Политики информационной безопасности предприятия.
6. Раскройте содержание раздела «Распределение ролей и обязанностей» Политики информационной безопасности предприятия.
7. Раскройте содержание раздела «Санкции» Политики информационной безопасности предприятия.
8. Раскройте содержание раздела «Дополнительная информация» Политики информационной безопасности предприятия.
9. Охарактеризуйте верхний, средний и нижний уровни политики информационной безопасности предприятия.
10. Опишите обязанности руководителей подразделений в реализации положений политики информационной безопасности предприятия.
11. Опишите обязанности администраторов локальных сетей в реализации положений политики информационной безопасности предприятия.
12. Опишите обязанности администраторов сервисов в реализации положений политики информационной безопасности предприятия.
13. Опишите обязанности пользователей в реализации положений политики информационной безопасности предприятия.
14. Раскройте компоненты политики информационной безопасности предприятия.
15. Раскройте содержание базовой политики безопасности предприятия.
16. Раскройте содержание руководства по архитектуре безопасности предприятия.
17. Перечислите группы специализированных политик безопасности.
18. Перечислите специализированные политики безопасности, затрагивающих значительное число пользователей.
19. Перечислите специализированные политики безопасности, затрагивающих конкретные технические области.
20. Раскройте содержание политики допустимого использования предприятия.

21. Раскройте содержание политики удаленного доступа предприятия.
22. Раскройте понятие «процедура безопасности».
23. Раскройте содержание процедуры реагирования на события.
24. Раскройте содержание процедуры управления конфигурацией.
25. Опишите требования к политикам безопасности предприятия.
26. Опишите этапы разработки политики безопасности предприятия.
27. Опишите этап анализа рисков.
28. Опишите компоненты архитектуры безопасности сети.

Тема №5. Принципы многоуровневой защиты корпоративной информации

1. Дайте определение понятию «корпоративная информационная система» (КИС).
2. Перечислите принципы построения КИС.
3. Опишите структурную схему КИС.
4. Перечислите этапы управления КИС.
5. Опишите функции уровней защиты КИС.
6. Опишите подсистему защиты приложений КИС.
7. Опишите подсистему защиты сетей КИС.
8. Опишите подсистему защиты серверов КИС.
9. Опишите подсистему защиты конечных пользователей КИС.
10. Дайте определение понятию «облачные вычисления».
11. Дайте определение понятию «облачный сервис».
12. Дайте определение понятию «данные как услуга».
13. Дайте определение понятию «коммуникации как услуга».
14. Дайте определение понятию «рабочее место как услуга».
15. Раскройте концепцию вычисления в «облаке».
16. Дайте определение понятию «частное облако».
17. Дайте определение понятию «облако общего пользования».
18. Дайте определение понятию «гибридное облако».
19. Раскройте архитектуру облачных серверов.
20. Перечислите основные характеристики «облачных» вычислений.
21. Раскройте сущность такой характеристики «облачных» вычислений, как «масштабируемость».
22. Раскройте сущность такой характеристики «облачных» вычислений, как «эластичность».
23. Раскройте сущность такой характеристики «облачных» вычислений, как «мультитенантность».
24. Раскройте сущность такой характеристики «облачных» вычислений, как «оплата за использование».
25. Раскройте сущность такой характеристики «облачных» вычислений, как «самообслуживание».
26. Перечислите, в чем преимущества «облачных» вычислений.
27. Перечислите, в чем недостатки «облачных» вычислений.
28. Перечислите требования к разработке архитектуры комплексной системы защиты информации.
29. Перечислите меры, методы комплексной системы защиты информации.
30. Опишите структуру комплексной системы защиты информации.
31. Опишите подсистему защиты информации от несанкционированного доступа.
32. Опишите подсистему криптографической защиты.
33. Опишите подсистему управления идентификацией и доступом.
34. Опишите подсистему обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей.
35. Опишите подсистему управления средствами защиты информации.

36. Опишите подсистему контроля использования информационных ресурсов.
37. Опишите подсистему межсетевого экранирования.
38. Опишите подсистему обнаружения и предотвращения вторжений.
39. Опишите подсистему защиты от вредоносных программ и спама.
40. Опишите подсистему контроля эффективности защиты информации.
41. Опишите подсистему мониторинга и управления инцидентами ИБ
42. Опишите подсистему обеспечения непрерывности функционирования средств защиты.

<u>Тема №6.</u> Технологии безопасности данных предприятия

1. Дайте определение понятия «шифр».
2. Дайте определение понятия «шифрование информации».
3. Дайте определение понятия «дешифрование информации».
4. Раскройте схему криптосистемы шифрования.
5. Дайте определение понятия «ключ шифрования».
6. Назовите классы криптосистем.
7. Дайте характеристику типам криптографических алгоритмов.
8. Дайте определение понятия «хеширование».
9. Раскройте особенности симметричного шифрования. Перечислите преимущества и недостатки данного типа шифрования.
10. Раскройте особенности блочного шифрования. Перечислите преимущества и недостатки данного типа шифрования. Раскройте понятия «рассеивание» и «перемешивание».
11. Раскройте особенности поточного шифрования. Перечислите преимущества и недостатки данного типа шифрования.
12. Раскройте особенности асимметричного шифрования. Перечислите преимущества и недостатки данного типа шифрования. Раскройте понятия «открытый ключ» и «секретный ключ».
13. Опишите порядок передачи зашифрованной информации в асимметричной криптосистеме.
14. Дайте определение понятия «электронная цифровая подпись» (ЭЦП). Назовите процедуры, которые включает система ЭЦП.
15. Опишите процедуру формирования ЭЦП.
16. Опишите процедуру проверки ЭЦП.
17. Опишите принципы функционирования открытых ключей PKI.
18. Раскройте понятия «сертификация открытого ключа», «удостоверяющий центр», «сертификат открытого ключа».
19. Раскройте составляющие и свойства сертификата открытого ключа.
20. Назовите типы сертификатов открытых ключей.
21. Опишите, что понимается под инфраструктурой открытых ключей PKI.
22. Назовите задачи использования открытых ключей PKI.
23. Дайте определение понятия «токен безопасности».
24. Опишите структуру открытых ключей PKI.
25. Назовите функции управления сертификатами открытых ключей.
26. Назовите функции управления ключами.
27. Дайте определение понятия «идентификация».
28. Дайте определение понятия «аутентификация».
29. Дайте определение понятия «авторизация».
30. Дайте определение понятия «администрирование».
31. Дайте определение понятия «пароль».
32. Дайте определение понятия «персональный идентификационный номер».
33. Дайте определение понятия «динамический (одноразовый) пароль».

34. Дайте определение понятия «система запрос-ответ».
35. Раскройте особенности процедуры простой аутентификации.
36. Раскройте особенности процедуры аутентификации на основе одноразовых паролей.
37. Раскройте особенности процедуры строгой аутентификации.
38. Раскройте особенности процедуры аутентификации на основе смарт-карт.
39. Раскройте особенности процедуры аутентификации на основе USB-токенов.
40. Дайте определение понятия «межсетевой экран».
41. Раскройте схему подключения межсетевого экрана.
42. Раскройте классификацию межсетевых экранов по функционированию на уровнях модели OSI.
43. Раскройте классификацию межсетевых экранов по используемой технологии.
44. Раскройте классификацию межсетевых экранов по исполнению.
45. Раскройте классификацию межсетевых экранов по схеме подключения.
46. Раскройте процедуру фильтрации трафика с помощью межсетевых экранов.
47. Опишите функцию посредничества, выполняемую межсетевыми экранами.
48. Раскройте особенности построения виртуальных защищенных сетей VNP.
49. Раскройте понятие «туннель VNP».
50. Раскройте понятие «VNP-клиент».
51. Раскройте понятие «шлюз безопасности VNP».
52. Раскройте понятие «VNP-сервер».
53. Раскройте особенности виртуального защищенного канала между локальными сетями.
54. Раскройте особенности виртуального защищенного канала между узлом и локальной сетью.

<u>Тема №7.</u> Защита от вредоносных программ и спама

1. Раскройте понятие «компьютерный вирус».
2. Раскройте жизненный цикл компьютерного вируса.
3. Перечислите виды компьютерных вирусов.
4. Раскройте технологии подготовки компьютерным вирусом своих копий.
5. Раскройте понятие «сетевой червь». Опишите виды данных компьютерных вирусов.
6. Раскройте понятие «троянский конь». Опишите виды данных компьютерных вирусов.
7. Раскройте понятие «шпионское программное обеспечение».
8. Раскройте понятие «условно опасные программы».
9. Опишите виды условно опасных программ.
10. Раскройте содержание сигнатурных методов обнаружения вредоносных программ.
11. Раскройте содержание проактивных методов обнаружения вредоносных программ.
12. Опишите особенности эвристических анализаторов.
13. Опишите особенности поведенческих блокираторов.
14. Перечислите дополнительные модули современных антивирусных программ.
15. Опишите модуль обновления современных антивирусных программ.
16. Опишите модуль планирования современных антивирусных программ.
17. Опишите модуль управления современных антивирусных программ.
18. Опишите технологию карантина современных антивирусных программ.
19. Перечислите режимы работы антивирусных программ.
20. Дайте определение «антивирусный комплекс».
21. Перечислите виды антивирусных комплексов.
22. Дайте определение «рабочие станции».
23. Дайте определение «сетевые серверы».
24. Дайте определение «почтовые системы».
25. Дайте определение «шлюз».
26. Перечислите дополнительные средства защиты в антивирусных программах.

27. Опишите особенности работы брендмауэров.
28. Опишите средства защиты от нежелательной корреспонденции.
29. Опишите особенности работы антивирусных облаков.
30. Перечислите преимущества и недостатки антивирусных облаков.

Тема №8. Управление средствами обеспечения информационной безопасности

1. Перечислите задачи управления информационной безопасностью.
2. Опишите основные подходы к решению проблемы организации взаимодействия и комплексирования традиционных систем управления КИС и систем управления информационной безопасностью.
3. Опишите решение задачи управления обновлениями программных средств.
4. Опишите решение задачи управления конфигурациями.
5. Опишите решение задачи разграничения доступа к сетевому оборудованию.
6. Дайте характеристику концепции глобального управления безопасностью GSM.
7. Перечислите принципы организации централизованного управления безопасностью КИС, согласно концепции глобального управления безопасностью GSM.
8. Раскройте структуру правила глобальной политики безопасности.
9. Раскройте понятие «политика по умолчанию».
10. Раскройте структурную схему системы управления средствами информационной безопасности.
11. Раскройте понятие «агент безопасности». Опишите его функции.
12. Раскройте понятие «центр управления GSM».
13. Раскройте понятие «консоль управления GSM».
14. Опишите решение задачи управления средствами защиты
15. Раскройте понятие «аудит безопасности».
16. Раскройте цели проведения аудита безопасности.
17. Перечислите этапы аудита безопасности.
18. Раскройте содержание этапа инициирования аудита безопасности.
19. Раскройте содержание этапа сбора информации аудита безопасности.
20. Раскройте содержание этапа анализа данных аудита безопасности.
21. Раскройте содержание этапа выработки рекомендаций аудита безопасности.
22. Раскройте содержание этапа подготовки отчетных документов аудита безопасности.
23. Раскройте содержание этапа результатов проведения аудита безопасности.
24. Раскройте особенности мониторинга безопасности информационной системы предприятия.

5.1.2. Методические рекомендации по подготовке к устному опросу

При подготовке к устному опросу следует, прежде всего, просмотреть конспекты лекций. Если какие-то вопросы вынесены преподавателем на самостоятельное изучение, следует обратиться к учебной литературе, рекомендованной преподавателем в качестве источника сведений.

5.1.3. Критерии оценивания при устном опросе

1) «отлично» (3 балла) – правильные ответы даны на 75-100% вопросов;
2) «хорошо» (2 балла) – правильные ответы даны на 51-75% вопросов;
3) «удовлетворительно» (1 балл) – если правильные ответы даны на 26-50% вопросов;
4) «неудовлетворительно» (0 баллов) – правильные ответы даны менее чем на 25% включительно.

5.1.4. Оценочные материалы для выполнения рефератов

Тема №1. Теоретические основы информационной безопасности предприятия

1. Основные понятия и термины в области информационной безопасности предприятия.
2. Определение информационной безопасности в свете информационных проблем современного общества.
3. Информация как объект права собственности. Объект защиты информации.
4. Проблемы развития теории и практики обеспечения информационной безопасности предприятия.
5. Основные составляющие информационной безопасности и их значение для субъектов информационных отношений.

Тема №2. Угрозы информационной безопасности экономических субъектов

1. Модель гипотетического нарушителя информационной безопасности предприятия.
2. Случайные и преднамеренные угрозы информационной безопасности предприятия.
3. Компьютерные преступления: понятие, виды и ответственность.
4. Компьютерные вирусы: понятие, виды и методы защиты.
5. Методы и технологии борьбы с вредоносными программами.
6. Основные положения методологии информационного противоборства.

Тема №3. Нормативно-правовые основы информационной безопасности и защиты информации предприятия

1. Конституция РФ об информационной безопасности. Стратегические и доктринальные документы в области информационной безопасности.
2. Законодательство РФ в области информационной безопасности.
3. Подзаконные акты РФ по вопросам информационной безопасности.
4. Роль стандартов информационной безопасности.
5. Международные стандарты информационной безопасности: стандарты ISO/IEC 17799:2002 (BS 7799:2000).
6. Международные стандарты информационной безопасности: германский стандарт BSI.
7. Международные стандарты информационной безопасности: стандарты ISO 15408 «Общие критерии безопасности информационных технологий».
8. Международные стандарты для беспроводных сетей: стандарт IEE 802.11/
9. Международные стандарты информационной безопасности для Интернета.
10. Отечественные стандарты безопасности информационных технологий.
11. Стандарт «Критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЕК 15408.
12. Закон РФ «О государственной тайне».

Тема №4. Политика информационной безопасности предприятия

1. Угрозы и уязвимости автоматизированных информационных систем.
2. Оценка уровня защищённости информационных систем.
3. Методы и средства технической защиты информации.
4. Особенности эксплуатации технических средств защиты информации.
5. Методы и средства защиты информации от традиционного шпионажа и диверсий.
6. Защита информации предприятия от несанкционированного доступа.

Тема №5. Принципы многоуровневой защиты корпоративной информации

1. Информационная безопасность автоматизированных систем.
2. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн).
3. Особенности защиты информации, составляющей коммерческую тайну компании.

4. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры.
5. Минимизация ущерба от аварий и стихийных бедствий. Дублирование информации.
6. Повышение надежности информационной системы. Создание отказоустойчивых информационных систем.
7. Оптимизация взаимодействия пользователей информационной системы предприятия и обслуживающего ее персонала.

Тема №6. Технологии безопасности данных предприятия

1. Криптографические методы защиты информации.
2. Современные симметричные и асимметричные криптографические системы.
3. Оценка криптостойкости шифров.
4. Правила работы с паролями.
5. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.
6. Методики обоснования выбора средств технической и криптографической защиты информации.
7. Системы предотвращения вторжений (IDS).

Тема №7. Защита от вредоносных программ и спама

1. Управление информационной безопасностью.
2. Организация конфиденциального делопроизводства.
3. Аудит информационной безопасности.
4. Экономика защиты информации.
5. Выбор, установка, настройка и эксплуатация средств антивирусной защиты.
6. Программные средства анализа рисков информационной безопасности.

Тема №8. Управление средствами обеспечения информационной безопасности

1. Понятие и объекты аттестации объектов информатизации по требованиям безопасности.
2. Нормативное регулирование аттестации объектов информатизации по требованиям безопасности информации.
3. Система аттестации объектов информатизации.
4. Органы аттестации объектов информатизации по требованиям безопасности информации.
5. Порядок аттестации объектов информатизации по требованиям безопасности информации.

5.1.5. Требования к структуре, содержанию, методические рекомендации по написанию реферата

Реферат подготавливается и оформляется с учетом требований ГОСТ 7.32 -2001.

Под рефератом подразумевается творческая исследовательская работа, основанная, прежде всего, на изучении значительного количества научной и иной литературы по теме исследования.

Требования к структуре и содержанию реферата:

Реферат, как правило должен содержать следующие структурные элементы:

- титульный лист;
- содержание;
- введение;
- текст реферата (основная часть);
- заключение;

- список использованных источников (список литературы);
- приложения (при необходимости).

Титульный лист реферата оформляется по требованиям, указанным ниже.

Содержание – перечень основных частей работы с указанием листов (страниц), на которых их помещают. Содержание должно отражать все материалы, представляемые к защите работы. Слово «Содержание» записывают в виде заголовка, симметрично тексту, с прописной буквы, без номера раздела. В содержании приводятся наименования структурных частей реферата, глав и параграфов его основной части с указанием номера страницы, с которой начинается соответствующая часть, глава, параграф.

Во введении необходимо обозначить обоснование выбора темы, ее актуальность, объект и предмет, цель и задачи исследования, описываются объект и предмет исследования, информационная база исследования и структура работы. Заголовок «Введение» записывают симметрично тексту с прописной буквы.

В тексте реферата (основной части) излагается сущность проблемы и объективные научные сведения по теме реферата, дается критический обзор источников, собственные версии, сведения, оценки. Содержание основной части должно точно соответствовать теме реферата и полностью ее раскрывать. Главы и параграфы реферата должны раскрывать описание решения поставленных во введении задач. Поэтому заголовки глав и параграфов, как правило, должны соответствовать по своей сути формулировкам задач реферата. Заголовка «ОСНОВНАЯ ЧАСТЬ» в содержании реферата быть не должно. Текст реферата должен содержать адресные ссылки на научные работы, оформленные в соответствии требованиям ГОСТ. Также обязательным является наличие в основной части реферата ссылок на использованные источники. Изложение необходимо вести от третьего лица («Автор полагает...») либо использовать безличные конструкции и неопределенно-личные предложения («На втором этапе исследуются следующие подходы…», «Проведенное исследование позволило доказать...» и т.п.).

Заключение должно содержать краткие выводы по результатам выполненной работы, оценку полноты решения поставленных задач, разработку рекомендаций по использованию результатов исследования.

Список литературы должен оформляться в соответствии с общепринятыми библиографическими требованиями и включать только использованные студентом публикации. Количество источников в списке определяется студентом самостоятельно, для реферата их рекомендуемое количество от 10 до 20. Сведения об источниках приводятся в соответствии с требованиями ГОСТ 7.1. ГОСТ 7.80. ГОСТ 7.82. 5.10.2. Список использованных источников должен включать библиографические записи на документы, ссылки на которые оформляют арабскими цифрами в квадратных скобках.

Требования по оформлению реферата:

1. Печатная форма – документ должен быть создан на компьютере, в программе Microsoft Word.

2. Объем реферата – не менее 10 страниц и не более 20 страниц машинописного текста (без учета титульного листа, списка ключевых слов, содержания, списка использованных источников и приложений). Распечатка производится на одной стороне листа. Формат стандартный – А4.

3. Поля страницы: левое – 30 мм, правое, верхнее, нижнее поля – по 20 мм.

4. Выравнивание текста – по ширине. Красная строка оформляется на одном уровне на всех страницах реферата. Отступ красной строки равен 1,25 см.

5. Шрифт основного текста – Times New Roman. Размер – 14 п. Цвет – черный. Интервал между строками – полуторный.

6. Названия глав прописываются полужирным (размер – 16 п.), подзаголовки также выделяют жирным (размер – 14 п.). Если заголовок расположен по центру страницы, точка в конце не ставится. Заголовок не подчеркивается. Названия

разделов и подразделов прописывают заглавными буквами. Каждый структурный элемент реферата начинается с новой страницы.

7. Между названием главы и основным текстом необходим интервал в 2,5 пункта. Интервал между подзаголовком и текстом – 2 п. Между названиями разделов и подразделов оставляют двойной интервал.

8. Нумерация страниц начинается с титульного листа, но сам титульный лист не нумеруется. Используются арабские цифры. Страницы нумеруются в нижнем правом углу без точек.

9. Примечания располагают на той же странице, где сделана сноска. Цитаты заключаются в скобки. Авторская пунктуация и грамматика сохраняется.

10. Главы нумеруются римскими цифрами (Глава I, Глава II), параграфы – арабскими (1.1, 1.2).

11. Титульный лист – в верхней части указывают полное название университета. Ниже указывают тип и тему работы. Используют большой кегль. Под темой, справа, размещают информацию об авторе и научном руководителе. В нижней части по центру – название города и год написания.

12. Список использованных источников должен формироваться в алфавитном порядке по фамилии авторов. Все источники нумеруются и располагаются в определенном порядке:

- законы;
- постановления Правительства;
- другая нормативная документация;
- статистические данные;
- научные материалы;
- газеты и журналы;
- учебники;
- электронные ресурсы.

Включенная в список литература нумеруется сплошным порядком от первого до последнего названия. По каждому литературному источнику указывается: автор (или группа авторов), полное название книги или статьи, место и наименование издательства (для книг и брошюр), год издания; для журнальных статей указывается наименование журнала, год выпуска и номер. По сборникам трудов (статей) указывается автор статьи, ее название и далее название книги (сборника) и ее выходные данные. Ссылки на интернет-ресурсы в реферате правильно оформлять в соответствии с указаниями ГОСТ 7.82.

13. В приложения рекомендуется включать материалы иллюстративного и вспомогательного характера. В приложения могут быть помещены: таблицы и иллюстрации большого формата; дополнительные расчеты. На все приложения в тексте работы должны быть даны ссылки. Приложения располагают в работе и обозначают в порядке ссылок на них в тексте. Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ь, Ы, Ъ. Например: «Приложение Б». Каждое приложение в работе следует начинать с нового листа (страницы) с указанием наверху посередине страницы слова «Приложение» и его обозначения. Приложение должно иметь заголовок, который записывают симметрично тексту с прописной буквы отдельной строкой.

5.1.6. Критерии оценивания при защите реферата

Максимальная оценка – 3 балла:

1. Соответствие содержания заявленной теме, отсутствие в тексте отступлений от темы – 0,5 баллов;
2. Логичность и последовательность в изложении материала – 0,5 баллов;
3. Способность к работе с литературными источниками, Интернет-ресурсами – 0,5 баллов;

4. Способность к анализу и обобщению информационного материала, степень полноты обзора состояния вопроса, обоснованность выводов – 1 балл;
5. Правильность оформления (соответствие стандарту, структурная упорядоченность, ссылки, цитаты, таблицы и т.д.) – 0,5 баллов.

5.1.7. Оценочные материалы для самостоятельной работы обучающегося (примеры практических работ)

Задание 1.

Цель практической работы: закрепление теоретического материала по теме №2. Угрозы информационной безопасности экономических субъектов.

Задачи практической работы: раскрыть содержание, каналы утечки информации, методы и средства получения информации, методы и средства защиты информации.

Содержание задания: Работа в малых группах. Вашей группе необходимо заполнить предложенную форму таблицы, определив:

А. Типовые каналы утечки информации.

Б. Методы инженерно-технической защиты компьютерной сети.

В. Технические средства противодействия утечки информации.

Составить аналитический отчет.

Таблица – Основные методы и средства несанкционированного получения информации и возможная защита от них

П/п	Действие (типовая ситуация)	Каналы утечки информации	Методы и средства получения информации	Методы и средства защиты информации
1	Разговор – в помещении, на улице			
2	Разговор по сотовому телефону			
3	Документ на бумажном носителе			
4	Изготовление документа на бумажном носителе			
5	Документ на небумажном носителе			
6	Изготовление документа на небумажном носителе			
7	Почтовое отправление			
8	Передача документа по каналу связи			
10	Производственный процесс			

Задание 2.

Цель практической работы: закрепление теоретического материала по теме №7. Защита от вредоносных программ и спама.

Задачи практической работы: определить основные функции, достоинства и недостатки современного антифирусного ПО.

Содержание задания: Работа в малых группах. Вашей группе необходимо заполнить предложенную форму таблицы, определив:

А. Основные функции предложенных пакетов антивирусных программ.

Б. Основные достоинства предложенных пакетов антивирусных программ.

В. Основные недостатки предложенных пакетов антивирусных программ.

Составить аналитический отчет.

.

Таблица – Антивирусное программное обеспечение

П/п	ПО	Функции ПО	Достоинства ПО	Недостатки ПО
1	Kaspresky Internet Security			
2	Advanced SystemCare Ultimate			
3	Avast Free			
4	Malware Fighter Pro			
5	BitDefender			
6	Nano Antivirus			
7	DrWeb			
8	MalwareBytes			
10	Avira Free Security Suite			
11	AVG			
12	360 Total Security			

5.1.8. Критерии оценивания практических работ

Предел длительности контроля	
Максимальное число баллов	3 балла
Критерии оценки	соответствие предполагаемым ответам – 1 балл
	правильное использование алгоритма выполнения действий (методики, технологии и т.д.) – 1 балл
	логика рассуждений, неординарность подхода к решению – 1 балл

5.2. Оценочные материалы для рубежного контроля. *Рубежный контроль* осуществляется по более или менее самостоятельным разделам – учебным модулям курса и проводится по окончании изучения материала модуля в заранее установленное время. Рубежный контроль проводится с целью определения качества усвоения материала учебного модуля в целом. В течение семестра проводится ***три таких контрольных мероприятия по графику***.

В качестве форм рубежного контроля используется тестирование (письменное или компьютерное), проведение коллоквиума. Выполняемые работы должны храниться на кафедре течении учебного года и по требованию предоставляться в Управление контроля качества. На рубежные контрольные мероприятия рекомендуется выносить весь программный материал (все разделы) по дисциплине.

5.2.1. Оценочные материалы для коллоквиума

6 семестр

Коллоквиум №1

1. Основные понятия информационной безопасности.
2. Взаимодействие основных субъектов и объектов обеспечения информационной безопасности.
3. Основные понятия защиты информации.
4. Меры и средства обеспечения информационной безопасности.
5. Анализ и классификация угроз информационной безопасности.
6. Анализ угроз в компьютерных сетях.
7. Угрозы безопасности и уязвимости в беспроводных сетях.
8. Криминализация атак на информационные системы.
9. Появление кибероружия для ведения кибервойн.
10. Нормативные акты, регулирующие сферу информационной безопасности в РФ.
11. Федеральный закон «Об информации, информационных технологиях и о защите информации».
12. Федеральный закон «О коммерческой тайне».

13. Федеральный закон «О персональных данных».
14. Ответственность за нарушения в сфере компьютерной информации.

Коллоквиум №2

1. Основные понятия политики информационной безопасности.
2. Структура политики информационной безопасности организации.
3. Базовая и специализированная политики информационной безопасности предприятия.
4. Процедуры обеспечения информационной безопасности предприятия.
5. Разработка политики информационной безопасности предприятия.
6. Компоненты архитектуры безопасности корпоративной сети.
7. Корпоративная система с традиционной структурой.
8. Системы облачных вычислений.
9. Многоуровневый подход к обеспечению информационной безопасности корпоративной информационной системы.
10. Подсистемы информационной безопасности традиционных корпоративных информационных систем.
11. Основные понятия криптографической защиты информации.
12. Электронная цифровая подпись.
13. Инфраструктура управления открытыми ключами PKI.
14. Аутентификация, авторизация и администрирование действий пользователей.
15. Технологии межсетевого экранирования.
16. Технологии виртуальных защищенных сетей VNP.

Коллоквиум №3

1. Классификация вредоносных программ.
2. Основы работы антивирусных программ.
3. Режимы работы антивирусных программ.
4. Облачная антивирусная технология.
5. Защита персональных компьютеров и корпоративных систем от действия вредоносных программ и вирусов.
6. Задачи управления информационной безопасностью.
7. Концепция глобального управления безопаснотью GSM.
8. Функционирование системы управления информационной безопасностью корпоративной информационной системы.
9. Аудит безопасности корпоративной информационной системы.
10. Мониторинг безопасности информационной системы компании.
11. Обзор современных систем управления безопасностью корпоративных информационных систем.
12. Обеспечение безопасности облачных технологий.

5.2.2. Методические рекомендации к подготовке к коллоквиуму

При подготовке к коллоквиуму следует, прежде всего, просмотреть конспекты лекций и практических занятий и отметить в них имеющиеся вопросы коллоквиума. Если какие-то вопросы вынесены преподавателем на самостоятельное изучение, следует обратиться к учебной литературе, рекомендованной преподавателем в качестве источника сведений.

5.2.3. Критерии оценивания при коллоквиуме

1) «отлично» (5-6 баллов) – правильные ответы даны на 75-100% вопросов;
2) «хорошо» (3-4 балла) – правильные ответы даны на 51-75% вопросов;
3) «удовлетворительно» (1-2 балла) – если правильные ответы даны на 26-50% вопросов;

4) «неудовлетворительно» (0 баллов) – правильные ответы даны менее чем на 25% включительно.

5.2.4. Оценочные материалы: Типовые тестовые задания по дисциплине «Информационная безопасность экономической деятельности»

1. К основным составляющим системы информационной безопасности относят
   a) Доступность информации
   b) Целостность информации
   c) Конфиденциальность информации
   d) Проверка прав доступа к информации
   e) Выявление нарушителей
2. Конфиденциальность информации обеспечивает
   a) Доступность информации только лицам, которым она предназначена
   b) Защищенность информации от потери
   c) Доступность информации только автору
   d) Нет верного ответа
3. Доступность информации обеспечивает
   a) Получение требуемой информации за определённый срок
   b) Защищенность информации от возможных угроз
   c) Неизменность информации в любое время
   d) Получение требуемой информации за неопределённый срок
4. Целостность информации обеспечивает
   a) Доступность информации только автору
   b) Защищенность информации от потери
   c) Существование информации в исходном виде
   d) Доступность информации определенному кругу пользователей
5. Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, потере целостности, конфиденциальности, доступности информации – это
   a) Угроза информационной безопасности
   b) Фальсификация информации
   c) Несанкционированный доступ к информации
   d) Нет верного ответа
6. Одной из задач информационной безопасности является
   a) Устранение последствий форс-мажорных событий
   b) Защита технических и программных средств от ошибочных действий пользователей
   c) Устранение неисправностей аппаратных средств
   d) Восстановление линий связи (в том числе телекоммуникационных)
7. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб пользователям информации – это
   a) Информационная безопасность
   b) Компьютерная безопасность
   c) Защита информации
   d) Защита государственной тайны
8. К составляющим системы информационной безопасности можно отнести
   a) Антивирусная защита
   b) Целостность информации
   c) Несанкционированный доступ к информации
   d) Санкционированный доступ к информации
   e) Выявление нарушителей

9. Совокупность методов и средств, предназначенных для ограничения доступа к ресурсам – это
   a) Сертификация
   b) Секретность
   c) Контроль доступа
   d) Нет верного ответа
10. Комплекс средств и методов, направленных на предотвращение угроз информационной безопасности и устранение их последствий – это
   a) Информационная безопасность
   b) Компьютерная безопасность
   c) Защита информации
   d) Защита государственной тайны
11. Процесс распознавания автоматизированной системой пользователя по его уникальному имени – это
   a) Идентификация
   b) Аутентификация
   c) Контроль доступа
   d) Сертификация
12. Процедура проверки подлинности информации, предъявленной пользователем, предназначенная для подтверждения истинности пользователя – это
   a) Идентификация
   b) Аутентификация
   c) Контроль доступа
   d) Сертификация
13. Присвоение субъектам идентификаторов и(или) сравнение предъявляемых идентификаторов с перечнем идентификаторов, владельцы которых допущены к информационной системе – это
   a) Идентификация
   b) Аутентификация
   c) Контроль доступа
   d) Аутентичность
   e) Конфиденциальность
14. Использование процедур идентификации и аутентификации преследует цели
   a) Повышения физической защиты информационной системы
   b) Ограничение доступа случайных и незаконных субъектов к информационной системе
   c) Защиты от компьютерных вирусов
   d) Обеспечение целостности данных
15. Основными направлениями защиты информации являются
   a) Предупреждение угроз
   b) Выявление угроз
   c) Ликвидация угроз
   d) Ликвидация последствий угроз
   e) Стабилизация угроз
   f) Регистрация угроз
16. Действия, направленные на устранение действующей угрозы и конкретных преступных действий – это
   a) Предупреждение угроз
   b) Выявление угроз
   c) Обнаружение угроз
   d) Ликвидация угроз
17. Действия, направленные на преодоление конкретной угрозы и ее источников,

приносящих тот или иной вид ущерба – это

a) Предупреждение угроз
b) Выявление угроз
c) Обнаружение угроз
d) Ликвидация угроз

18. Проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке – это

a) Предупреждение угроз
b) Выявление угроз
c) Обнаружение угроз
d) Ликвидация угроз

19. Информация, несанкционированное копирование, хищение, разглашение (распространение, опубликование), модификация, уничтожение или использование которой может нанести существенный моральный или материальный ущерб ее собственному или владельцу, а также третьей стороны, интересы которой данная информация затрагивает, называется

a) Критичной информацией
b) Информацией общего доступа
c) Персональными данными
d) Конфиденциальными данными

20. Категориями ценности информации с точки зрения информационной безопасности являются

a) Конфиденциальность
b) Целостность
c) Статичность
d) Аутентичность
e) Адекватность
f) Доступность
g) Аппелируемость

21. Гарантия того, что источником информации является именно то лицо, которое заявлено как автор информации – это категория

a) Аутентичность
b) Аппелируемость
c) Достоверность
d) Статичность

22. Аутентичность предполагает

a) Проверку прав доступа
b) Доказательство авторства документа
c) Изменение авторства документа
d) Контроль целостности данных

23. Гарантия того, что при необходимости можно доказать, что автором сообщения является указанный человек и не может являться никто другой – это

a) Аутентичность
b) Аппелируемость
c) Достоверность
d) Статичность

24. Убытки, которые могут возникнуть вследствие внесения изменений в информацию, если факт модификации не был обнаружен – это

a) Стоимость утраты
b) Стоимость скрытого нарушения целостности
c) Стоимость потери конфиденциальности

d) Нет верного ответа

25. Потенциальные убытки, которые понесет владелец информации, если к ней получат несанкционированный доступ сторонние лица – это
    a) Стоимость утраты
    b) Стоимость скрытого нарушения целостности
    c) Стоимость потери конфиденциальности
    d) Нет верного ответа
26. Ущерб полного или частичного разрушения информации – это
    a) Стоимость утраты
    b) Стоимость скрытого нарушения целостности
    c) Стоимость потери конфиденциальности
    d) Нет верного ответа
27. К конфиденциальным сведениям относят
    a) Персональные данные граждан
    b) Сведения, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайны и пр.)
    c) Сведения о сущности изобретения до момента официальной публикации о них
    d) Сведения, полученные из внешних открытых источников
    e) Сведения, полученные на веб-сайте компании
    f) Сведения, подписанные руководством, для передачи вовне (конференции, презентации и пр.)
28. Не является преднамеренным воздействием на информационную систему
    a) Подбор пароля
    b) Хищение информации
    c) Перехват информации
    d) Модификация информации
29. Не является причиной случайных воздействий на информационную систему
    a) Подбор пароля
    b) Ошибки пользователей
    c) Отказы и сбои аппаратуры
    d) Помехи в линиях связи из-за воздействий внешней среды
30. Пути несанкционированной передачи информации
    a) Негласный просмотр информации, отображенной на мониторе
    b) Хищение носителей информации
    c) Подключение к устройствам передачи, обработки и хранения информации
    d) Внедрение резидентных программ
    e) Установка прослушивающих и передающих устройств
    f) Распространение информации ее владельцем
    g) Регистрация и анализ побочных электромагнитных излучений компьютерной техники, средств связи и телекоммуникаций
31. Реализация угроз информационной безопасности может привести к
    a) Уничтожению средств ввода-вывода информации
    b) Несанкционированному доступу к информации
    c) Изменению конфигурации периферийных устройств
    d) Нет верного ответа
32. Результатом реализации угрозы перехвата может стать
    a) Нарушение доступности данных
    b) Отказ в обслуживании
    c) Нарушение конфиденциальности данных
    d) Изменение конфигурации периферийных устройств
33. При разработке модели нарушителя определяются такие предположения
    a) О категориях лиц, к которым может принадлежать нарушитель

b) О мотивах действий нарушителя
c) О квалификации нарушителя и его технической оснащенности
d) О способности личности исполнять данную социальную роль
e) О характере возможных действий нарушителя

34. Уголовно наказуемые общественно опасные действия, в которых машинная информация является объектом посягательства – это
a) Компьютерное преступление
b) Несанкционированное действие
c) Компьютерное мошенничество
d) Кража

35. Любая программа, написанная с целью нанесения ущерба или использования ресурсов атакуемого компьютера – это
a) Вредоносная программа
b) Компьютерный вирус
c) Программа закладка
d) Троянский конь

36. Жизненный цикл вируса состоит из этапов
a) Внедрение (инфицирование)
b) Инкубационный период
c) Выполнение специальных функций
d) Саморазмножение (репродуцирование)
e) Проявление

37. Интернет-мошенничество, целью которого является получение доступа к конфиденциальным данным пользователей (логинам, паролям) – это
a) Фишинг
b) Кардинг
c) Фарминг
d) Скимминг

38. Программа, скрытно внедренная в защищенную систему и позволяющая злоумышленнику путём модификации свойств системы защиты, осуществлять несанкционированный доступ к ресурсам системы – это
a) Программа-закладка
b) Троянская программа
c) Стелс-вирус
d) Нет верного ответа

39. Укажите методы обнаружения компьютерных вирусов
a) Сканирование
b) Обнаружение изменений
c) Эвристический анализ
d) Использование резидентных сторожей
e) Гаммирование
f) Аналитическое преобразование
g) Вакцинация
h) Аппаратно-программные антивирусные средства

40. Комплекс программных и аппаратных средств, осуществляющих контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами, позволяющих блокировать нежелательный сетевой трафик и обеспечивать невидимость ПК в сети с целью предотвращения кибер атак – это
a) Сетевой экран (firewall)
b) Маршрутизатор
c) Интернет-шлюз
d) Концентратор

41.Основополагающими документами по информационной безопасности в РФ являются
a) Конституция РФ
b) Концепция национальной безопасности
c) Уголовный кодекс РФ
d) Закон об информационной безопасности

42. Документ, гарантирующий: тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; право свободно искать, получать, передавать, производить и распространять информацию любым законным способом; свободу массовой информации – это
a) Конституция РФ
b) Концепция национальной безопасности
c) Уголовный кодекс РФ
d) Закон об информационной безопасности

43. Документ, определяющий важнейшие задачи обеспечения информационной безопасности РФ – это
a) Конституция РФ
b) Концепция национальной безопасности
c) Уголовный кодекс РФ
d) Закон об информационной безопасности

44. Документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности – это
a) Конфиденциальная информация
b) Персональные данные
c) Государственная тайна
d) Служебная тайна

45. Информация, с помощью которой можно однозначно идентифицировать физическое лицо – это
a) Конфиденциальная информация
b) Персональные данные
c) Государственная тайна
d) Служебная тайна

46. В политике безопасности предприятия не рассматривается
a) Требуемый уровень защиты данных
b) Анализ рисков
c) Защищенность сотрудников
d) Роли субъектов информационных отношений

47. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов – это
a) Политика безопасности
b) Информационная политика
c) Информационная безопасность
d) Защита информации

48. Стратегия организации в области информационной безопасности, мера внимания и количество ресурсов, которые руководство компании считает целесообразным выделить для обеспечения информационной безопасности – это
a) Политика безопасности
b) Стратегия безопасности
c) Концепция безопасности
d) Нет верного ответа

49. Политика безопасности разрабатывается на уровне обеспечения информационной безопасности

a) Информационном
b) Административном
c) Законодательно-правовом
d) Программно-техническом

50. Административный уровень обеспечения информационной безопасности не определяет
a) Разработку политики безопасности
b) Проведения анализа угроз и расчета рисков
c) Выбор механизмов обеспечения информационной безопасности
d) Внедрение механизмов безопасности

51. Комплекс мероприятий, реализующих практические механизмы защиты информации, реализуется на уровне обеспечения информационной безопасности
a) Информационном
b) Административном
c) Законодательно-правовом
d) Программно-техническом
e) Процедурном

52. Этот уровень не относится к уровням обеспечения информационной безопасности
a) Информационный
b) Административный
c) Законодательно-правовой
d) Программно-технический

53. Методы организации разграничения доступа к информации в информационных системах
a) Матричный
b) Реляционный
c) Полномочный (мандатный)

54. Способы преобразования при шифровании
1. Подстановка
2. Перестановка
3. Аналитическое преобразование
4. Кодирование
5. Гаммирование

55. В криптосистему не входит
a) Алгоритм шифрования
b) Полиморфик-генератор
c) Система управления ключами
d) Нет верного ответа

56. При асимметричном шифровании для шифрования и расшифровки используются
a) Два взаимосвязанных ключа
b) Один открытый ключ
c) Два открытых ключа
d) Один закрытый ключ

57. Цифровая подпись не обеспечивает
a) Контроль целостности документа
b) Конфиденциальность документа
c) Доказательное подтверждение авторства документа
d) Восстановление поврежденного документа

58. Программные модули или аппаратные устройства, регистрирующие каждое нажатие клавиши на клавиатуре компьютера
a) Скриншоты
b) Кайлотеры

c) Брандмауэры
d) Браузеры

59. Размер ключа в ГОСТ 28147-89
    a) 128 бит
    b) 56 бит
    c) 64 бит
    d) 256 бит

60. Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и(или) выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации – это
    a) Межсетевой экран
    b) Крипто-алгоритм
    c) Криптосистема
    d) Сервер удаленного доступа

61. Типы межсетевых экранов
    a) Межсетевые экраны прикладного уровня
    b) Гибридные межсетевые экраны
    c) Межсетевые экраны с пакетной фильтрацией
    d) Релевантные межсетевые экраны

62. Ключевые компоненты виртуальной сети VNP
    a) Сервер VNP
    b) Алгоритмы шифрования
    c) Система аутентификации
    d) Система документирования
    e) Протокол VNP

63. Характеристиками виртуальных частных сетей являются
    a) Трафик шифруется для обеспечения защиты от прослушивания
    b) Осуществляется аутентификация удаленного сайта
    c) Обеспечивается поддержка множества протоколов
    d) Соединение обеспечивает связь только между двумя конкретными абонентами
    e) Трафик дешифруется для обеспечения защиты от прослушивания

64. Цели применения системы предотвращения атак – IDS
    a) Обнаружение атак
    b) Предотвращение атак
    c) Обнаружение нарушений политик безопасности
    d) Принуждение к использованию политик безопасности
    e) Принуждение к следованию политикам безопасности
    f) Сбор доказательств нарушений безопасности
    g) Шифрование и дешифрование трафика

65. Основные типы систем предотвращения атак – IDS
    a) Узловые
    b) Сетевые
    c) Протокольные
    d) Все перечисленные

5.2.5. Методические рекомендации к тестированию

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся эталоны ответов.

При самостоятельной подготовке к тестированию студенту необходимо:

1. Готовясь к тестированию, проработать информационный материал по дисциплине, получить консультацию преподавателя по вопросу выбора учебной литературы;

2. Выяснить все условия тестирования заранее: сколько тестов будет предложено; сколько времени отводится на тестирование; какова система оценки результатов и т.д.
3. При работе с тестами, необходимо внимательно и до конца прочитать вопрос и предлагаемые варианты ответов. Выбрать правильные (их может быть несколько). На отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам;
4. В процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант;
5. Если встретился трудный вопрос, не следует тратить много времени на него, лучше перейти к другим тестам и вернуться к трудному вопросу в конце.
6. Обязательно следует оставить время для проверки ответов, чтобы избежать механических ошибок.

5.2.6. Критерии оценивания

Предел длительности контроля	30 мин
Предлагаемое количество заданий из одного контролируемого подраздела	20-25 тестовых заданий
Критерии оценки	
«4 балла», если	76-100%
«3 балла», если	51-75%
«2 балла», если	26-50%
«1 балл», если	11-25%
«0 баллов», если	0-10%

5.3. Оценочные материалы для промежуточной аттестации. *Целью промежуточных аттестаций* по дисциплине является оценка качества ее освоения студентами.

Промежуточная аттестация предназначена для объективного подтверждения и оценивания достигнутых результатов обучения после завершения изучения дисциплины. Осуществляется в конце семестра и представляет собой итоговую оценку знаний по дисциплине «Информационная безопасность экономической деятельности» в виде проведения экзамена.

Промежуточная аттестация может проводиться в устной, письменной форме, и в форме тестирования. На промежуточную аттестацию отводится до 30 баллов на экзамене.

ВОПРОСЫ, ВЫНОСИМЫЕ НА ЭКЗАМЕН

1. Основные понятия информационной безопасности.
2. Взаимодействие основных субъектов и объектов обеспечения информационной безопасности.
3. Основные понятия защиты информации.
4. Меры и средства обеспечения информационной безопасности.
5. Анализ и классификация угроз информационной безопасности.
6. Анализ угроз в компьютерных сетях.
7. Угрозы безопасности и уязвимости в беспроводных сетях.
8. Криминализация атак на информационные системы.
9. Появление кибероружия для ведения кибервойн.
10. Нормативные акты, регулирующие сферу информационной безопасности в РФ.
11. Федеральный закон «Об информации, информационных технологиях и о защите информации».
12. Федеральный закон «О коммерческой тайне».
13. Федеральный закон «О персональных данных».
14. Ответственность за нарушения в сфере компьютерной информации.

15. Основные понятия политики информационной безопасности.
16. Структура политики информационной безопасности организации.
17. Базовая и специализированная политики информационной безопасности предприятия.
18. Процедуры обеспечения информационной безопасности предприятия.
19. Разработка политики информационной безопасности предприятия.
20. Компоненты архитектуры безопасности корпоративной сети.
21. Корпоративная система с традиционной структурой.
22. Системы облачных вычислений.
23. Многоуровневый подход к обеспечению информационной безопасности корпоративной информационной системы.
24. Подсистемы информационной безопасности традиционных корпоративных информационных систем.
25. Основные понятия криптографической защиты информации.
26. Электронная цифровая подпись.
27. Инфраструктура управления открытыми ключами PKI.
28. Аутентификация, авторизация и администрирование действий пользователей.
29. Технологии межсетевого экранирования.
30. Технологии виртуальных защищенных сетей VNP.
31. Классификация вредоносных программ.
32. Основы работы антивирусных программ.
33. Режимы работы антивирусных программ.
34. Облачная антивирусная технология.
35. Защита персональных компьютеров и корпоративных систем от действия вредоносных программ и вирусов.
36. Задачи управления информационной безопасностью.
37. Концепция глобального управления безопаснотью GSM.
38. Функционирование системы управления информационной безопасностью корпоративной информационной системы.
39. Аудит безопасности корпоративной информационной системы.
40. Мониторинг безопасности информационной системы компании.
41. Обзор современных систем управления безопасностью корпоративных информационных систем.
42. Обеспечение безопасности облачных технологий.

5.3.2. Примеры типовых контрольных заданий на экзамене

Цель контрольных заданий: формирование практических навыков по диагностике и обеспечению информационной безопасности экономической деятельности предприятий.

Задачи контрольных заданий: закрепление теоретических знаний о сущности базовых категорий информационной безопасности предприятия; формирование практических навыков работы с нормативно-правовой базой, регулирующей вопросы обеспечения информационной безопасности экономической и финансовой деятельности субъектов хозяйствования; формирование навыков разработки типовых мероприятий по обеспечению информационной безопасности и защите информации; формирование навыков анализа информационных ресурсов по факторам важности, конфиденциальности, уязвимости.

КОНТРОЛЬНОЕ ЗАДАНИЕ 1.

На предприятии широко используются информационные технологии. Для обеспечения информационной безопасности кадровой службе дано указание: разработать комплекс организационных мероприятий. Вы, как руководитель кадровой службы, должны:

А. Сформулировать концепцию информационной безопасности предприятия.

Б. Определить основные задачи системы информационной безопасности предприятия.

В. Сформулировать первоочередные меры по обеспечению информационной безопасности предприятия.

Г. Составить аналитический отчет.

КОНТРОЛЬНОЕ ЗАДАНИЕ 2.

На предприятии произошла крупная авария, связанная с ошибкой в программном обеспечении производственного процесса. Установите (в соответствии с действующим законодательством), кто будет отвечать за случившуюся аварию. Какой будет его ответственность. Составьте аналитический отчет.

КОНТРОЛЬНОЕ ЗАДАНИЕ 3.

Работник обратился в суд по поводу нарушения сотрудниками отдела кадров предприятия его права на защиту персональной информации (зафиксирована утечка сведений персонального характера).

Оцените ситуацию, определите виновных и причины.

Разработайте меры по предотвращению подобных ситуаций. Составьте аналитический отчет.

КОНТРОЛЬНОЕ ЗАДАНИЕ 4.

Организация работает с информацией, составляющей государственную тайну, и информацией, являющейся коммерческой тайной. Дайте сравнительную характеристику государственной и коммерческой тайн.

Предложите мероприятия по защите:

А. Государственной тайны;

Б. Коммерческой тайны.

Составьте аналитический отчет.

КОНТРОЛЬНОЕ ЗАДАНИЕ 5.

1. Выберите три различных информационных актива, используемых в офисе страховой организации.
2. На основе изучения Приложения D ГОСТа Р ИСО/МЭК ТО 13335-3-2007 подберите три конкретных уязвимости системы защиты данных информационных активов.
3. Пользуясь Приложением С ГОСТа Р ИСО/МЭК ТО 13335-3-2007 напишите три угрозы, реализация которых возможна, пока в системе не устранены названные уязвимости.
4. Пользуясь четвертым методом оценки риска, предложенным в Приложении Е ГОСТа, произведите оценку рисков информационной безопасности.
5. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.
6. Составьте аналитический отчет.

5.3.3. Критерии оценивания при экзамене

Оценка выполнения практического задания	до 15 баллов
Оценка собеседования по теоретической части	до 15 баллов
Критерии оценки (результат определяется как сумма всех составляющих)	
«Отлично» (91-100 баллов)	Выполнение практической части: – задание выполнено в полном объеме (95-100%) с соблюдением необходимой последовательности действий; – без ошибок выполнены все записи, таблицы, рисунки,

	вычисления; – проявлен высокий уровень умений применять знания и методы для решения практических задач/заданий; – владеет навыками использования полученных теоретических знаний и практических умений в сфере профессиональной деятельности. Собеседование по теоретической части: – в соответствии с паспортом компетенции показывает глубокое и полное знание категорий; – демонстрирует понимание важности приобретенных знаний и умений для будущей профессиональной деятельности.
«Хорошо» (81-90 баллов)	Выполнение практической части: – задание выполнено в объеме 85-95% с соблюдением необходимой последовательности действий; – без существенных ошибок выполнены все записи, таблицы, рисунки, вычисления; – проявлен достаточный уровень умений применять знания и методы для решения практических задач/заданий; – проявлено владение некоторыми навыками использования полученных теоретических знаний и практических умений в сфере профессиональной деятельности. Собеседование по теоретической части: – демонстрирует знание основных категорий, но допускает неточности в их объяснении; – демонстрирует понимание приобретенных знаний и умений для будущей профессиональной деятельности.
«Удовлетворительно» (61-80 баллов)	Выполнение практической части: – задание выполнено в объеме 60-85%, может быть нарушена последовательность действий, что не должно приводить к существенным ошибкам и неверным выводам; – без грубых ошибок выполнены записи, таблицы, рисунки, вычисления; – проявлен удовлетворительный уровень умений применять знания и методы для решения практических задач/заданий; – может с трудом показать навыки использования полученных знаний в будущей профессиональной деятельности. Собеседование по теоретической части: – имеет представление о категориях, но испытывает сложности при выборе методов объяснения их; – демонстрирует недостаточное понимание приобретенных знаний и умений для будущей профессиональной деятельности.
«Неудовлетворительно» (менее 61 балла)	Выполнение практической части: – задание выполнено в объеме менее 60%, нарушена последовательность действий, что привело к существенным ошибкам и неверным выводам; – с грубыми ошибками выполнены записи, таблицы, рисунки, вычисления; – проявлен неудовлетворительный уровень умений применять знания и методы для решения практических задач/заданий; – не может показать навыки использования полученных знаний в будущей профессиональной деятельности. Собеседование по теоретической части: – не имеет представления о категориях, испытывает сложности при выборе методов объяснения их; – демонстрирует непонимание приобретенных знаний и умений для будущей профессиональной деятельности.

Курсовая работа (проект) по дисциплине «Информационная безопасность экономической деятельности» не предусмотрены рабочим планом по направлению

38.03.01 Экономика, профиль «Информационно-аналитическое и правовое обеспечение экономической безопасности бизнеса».

6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Таблица 7. Результаты освоения учебной дисциплины, подлежащие проверке

Результаты обучения (компетенции)	***Основные показатели оценки результатов обучения***	***Вид оценочного материала, обеспечивающие формирование компетенций***
ПК-7 - способность, используя отечественные и зарубежные источники информации, собрать необходимые данные, проанализировать их и подготовить информационный обзор и/или аналитический отчет.	***Знать:*** – основные понятия, угрозы и нормативно-правовую базу в области информационной безопасности деятельности предприятия; – технологии обеспечения безопасности данных предприятия и защиты от вредоносных программ и спама; – принципы многоуровневой защиты корпоративной информации и управления средствами обеспечения информационной безопасности организации.	Типовые оценочные материалы для устного опроса (раздел 5.1.1); Типовые тестовые задания (раздел 5.2.4); Примерные темы рефератов (раздел 5.1.4); Типовые оценочные материалы при коллоквиуме (раздел 5.2.1); Типовые оценочные материалы к экзамену (раздел 5.3).
	Уметь: – осуществлять поиск, классификацию и первичную обработку информации для целей обеспечения информационной безопасности деятельности предприятия; – применять методы подготовки информационных и аналитических отчетов; – готовить презентации по результатам подготовленного информационного или аналитического материала.	Оценочные материалы для самостоятельной работы (практические задачи) (раздел 5.1.7); Примерные темы рефератов (раздел 5.1.4); Типовые тестовые задания (раздел 5.2.4).
	Владеть: – способами обработки, систематизации, оценки и интерпретации информации для целей обеспечения информационной безопасности деятельности предприятия; – современными методами оценки информации в сфере информационных технологий и защиты информации; навыками публичной презентации информационно-аналитических материалов и полемики по ним.	Оценочные материалы для самостоятельной работы (практические задачи) (раздел 5.1.7).

7. Учебно-методическое обеспечение дисциплины (модуля)

7.1. Нормативно-законодательные акты

1. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации». – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.
2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ. – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru. 3.
3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ. – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.
4. Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ. – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.

7.2. Основная литература

1. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов-бакалавров укрупненной группы направлений подготовки 38.00.00 «Экономика и управление» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 82 c. — 978-5-4487-0300-3. — Режим доступа: http://www.iprbookshop.ru/77319.html
2. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 c. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html
3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

7.3. Дополнительная литература

1. Филиппов Б.И. Информационная безопасность. Основы надежности средств связи [Электронный ресурс] : учебник / Б.И. Филиппов, О.Г. Шерстнева. — Электрон. текстовые данные. — Саратов: Ай Пи Эр Медиа, 2019. — 227 c. — 978-5-4486-0485-0. — Режим доступа: http://www.iprbookshop.ru/80290.html
2. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 c. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html
3. Морозов А.В. Информационное право и информационная безопасность. Часть 1 [Электронный ресурс] : учебник для магистров и аспирантов / А.В. Морозов, Л.В. Филатова, Т.А. Полякова. — Электрон. текстовые данные. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 436 c. — 978-5-00094-296-3. — Режим доступа: http://www.iprbookshop.ru/72395.html
4. Морозов А.В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс] : учебник для магистров и аспирантов / А.В. Морозов, Л.В. Филатова, Т.А. Полякова. — Электрон. текстовые данные. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 c. — 978-5-00094-297-0. — Режим доступа: http://www.iprbookshop.ru/66771.html
5. Горюхина Е.Ю. Информационная безопасность [Электронный ресурс] : учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. — Электрон. текстовые данные. — Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. — 221 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/72672.html

7.4. Периодические издания (журналы)

1. Информационные технологии – чит. зал №3.
2. Информационные ресурсы в России – чит. зал №3.

7.5. Интернет-ресурсы

1. Научная электронная библиотека «Киберленинка»: https://cyberleninka.ru/
2. СПС «КонсультантПлюс»: http://www.consultant.ru/
3. СПС «Гарант»: http://www.garant.ru/

7.6. Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы

Методические рекомендации при работе над конспектом во время проведения лекции

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются общие и утвердившиеся в практике правила, и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Целесообразно записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому обучающемуся необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

Методические рекомендации по подготовке к практическим занятиям

Практические (семинарские) занятия – составная часть учебного процесса, групповая форма занятий при активном участии обучающихся. Практические занятия способствуют углубленному изучению наиболее сложных проблем науки и служат основной формой подведения итогов самостоятельной работы обучающихся. Целью практических занятий является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к практическому занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем практические задания. При этом учесть рекомендации преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы.

Желательно при подготовке к практическим занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

На практических занятиях обучающиеся учатся грамотно излагать проблемы, свободно высказывать свои мысли и суждения, рассматривают ситуации, способствующие развитию профессиональной компетентности. Следует иметь в виду, что подготовка к практическому занятию зависит от формы, места проведения семинара, конкретных заданий и поручений. Это может быть написание реферата (с последующим их обсуждением), коллоквиум.

Методические рекомендации по организации самостоятельной работы

Организация самостоятельной работы по дисциплине включает следующее компоненты:

1. Самостоятельное изучение тем дисциплины;
2. Подготовка рефератов по предложенным темам;
3. Самоподготовку обучающихся к занятиям.

Самостоятельная работа обучающихся включает:

– изучение основной и дополнительной литературы;

– изучение материалов периодической печати и электронных ресурсов;
– подготовку к практическим занятиям;
– выполнение задания и подготовку к его защите;
– изучение проблемных ситуаций, не имеющих однозначного решения;
– подготовку к экзамену;
– индивидуальные и групповые консультации по наиболее сложным вопросам дисциплины.

Методические рекомендации по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой необходимо учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность студенту сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов обучающийся будет задавать к этим текстам вопросы. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью *изучающего* чтения является глубокое и всестороннее понимание учебной информации. Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.
2. Прием постановки вопросов к тексту имеет следующий алгоритм:
   - медленно прочитать текст, стараясь понять смысл изложенного;
   - выделить ключевые слова в тексте;
   - постараться понять основные идеи, подтекст и общий замысел автора.
3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Методические рекомендации по написанию рефератов

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами. Написание реферата используется в учебном процессе в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т.п. Процесс написания реферата включает: выбор темы; подбор нормативных актов, специальной литературы и иных источников, их изучение; составление плана; написание текста работы и ее оформление; устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов. Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве. Обучающийся при желании может сам предложить ту или иную тему, предварительно согласовав ее с научным руководителем.

Содержание реферата обучающийся докладывает на семинаре, кружке, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 7 - 10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения студенту выставляется соответствующая оценка.

8. Материально-техническое обеспечение дисциплины

Минимально необходимый для реализации ОПОП перечень материально-технического обеспечения включает в себя: лекционные аудитории – аудитории 307, 408, 409, 201, 213 ИПЭиФ (оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном и имеющие выход в сеть Интернет), помещения для проведения семинарских и практических занятий (оборудованные учебной мебелью), компьютерные классы (аудитории 304, 305, 403) и др.

По дисциплине имеются учебно-наглядные пособия в виде презентаций по всем темам, обеспечивающие тематические иллюстрации.

При проведении занятий лекционного типа, семинарских занятий используются:

лицензионное программное обеспечение:

– Продукты Microsoft (Desktop EducationALNG LicSaPk OLVS Academic Edition Enterprise) подписка (Open Value Subscription);

– Антивирусное программное обеспечение Kaspersky Endpoint Security Стандартный Russian Edition;

– Справочно-правовая система КонсультантПлюс.

свободно распространяемые программы:

– Academic MarthCAD License - математическое программное обеспечение, которое позволяет выполнять, анализировать важнейшие инженерные расчеты и обмениваться ими;

– WinZip для Windows - программ для сжатия и распаковки файлов;

– Adobe Reader для Windows – программа для чтения PDF файлов;

– Far Manager – консольный файловый менеджер для операционных систем семейства Microsoft Windows.

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается: 1. Альтернативной версией официального сайта в сети «Интернет» для слабовидящих; 2. Присутствие ассистента, оказывающего обучающемуся необходимую помощь; 3.Для инвалидов и лиц с ограниченными возможностями здоровья по слуху – дублирование вслух справочной информации о расписании учебных занятий; обеспечение надлежащими звуковыми средствами воспроизведения информации; 4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекту питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).

Приложение 1

ЛИСТ ИЗМЕНЕНИЙ (ДОПОЛНЕНИЙ)

в рабочую программу по дисциплине «Информационная безопасность экономической деятельности» по направлению подготовки 38.03.01 – Экономика; Профиль Информационно-аналитическое и правовое обеспечение экономической безопасности бизнеса на _____ учебный год

№п/п	Элемент (пункт) РПД	Перечень вносимых изменений (дополнений)	Примечание

Обсуждена и рекомендована на заседании кафедры экономики и финансов протокол № ____ от "___" _____ 20___г.

Заведующий кафедрой _____ / /