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 экономики и учетно-аналитических информационных систем

СОГЛАСОВАНО

Руководитель образовательной

программы _____ **Г.А. Эфендиева**

«30» января 2023 г.

УТВЕРЖДАЮ

Директор института

_____ **Е.М. Машукова**

«30» января 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ»

Специальность

38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Специализация

Экономико-правовое обеспечение экономической безопасности

Квалификация выпускника

Экономист

Форма обучения

Очная

Нальчик 2023

Рабочая программа дисциплины (модуля) «Информационная безопасность экономической деятельности» /сост. А.М. Губачиков – *Нальчик: КБГУ, 2023. – 52 с.*

Рабочая программа дисциплины (модуля) предназначена для студентов *очной* формы обучения по специальности 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности», 8 семестра, 4 курса.

Рабочая программа составлена с учетом федерального государственного образовательного стандарта высшего образования – специалитета по специальности 38.05.01 Экономическая безопасность, утвержденного приказом Минобрнауки России от 14.04.2021 г. № 293 (Зарегистрировано в Минюсте России 24.05.2021 г. № 63581).

С О Д Е Р Ж А Н И Е

1. Цели и задачи освоения дисциплины (модуля)

Целью изучения дисциплины «Информационная безопасность экономической деятельности» является освоение теоретических знаний и формирование практических навыков по диагностике и обеспечению информационной безопасности экономической деятельности предприятий.

Задачи изучения дисциплины «Информационная безопасность экономической деятельности»:

– знать сущность базовых категорий информационной безопасности предприятия;

– знать нормативно-правовую базу, регулирующую вопросы обеспечения информационной безопасности экономической и финансовой деятельности субъектов хозяйствования;

– сформировать умение определять мероприятия по обеспечению информационной безопасности и защите информации при осуществлении экономической деятельности хозяйствующих субъектов;

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

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина Б1.В.ДВ.05.02 «Информационная безопасность экономической деятельности» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули) ОПОП ВО по специальности 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности».

Изучение дисциплины «Информационная безопасность экономической деятельности» базируется на сумме знаний, полученных обучающимися в ходе освоения следующих дисциплин: «Бухгалтерские информационные системы», «Правовое обеспечение интеллектуальной и промышленной собственности», «Практикум по обеспечению экономической безопасности организаций», «Экономическая безопасность», «Конкурентное право и антимонопольное регулирование», «Цифровые информационно-коммуникационные технологии и искусственный интеллект», «Особенности выявления и расследования экономических и налоговых преступлений» и др.

Для освоения данной дисциплины, студенты должны владеть следующими знаниями: уметь использовать нормативно-правовые документы, иметь навыки анализа; уметь работать с информацией из различных источников. Успешное освоение данной дисциплины возможно только при комплексном изучении указанных областей знаний, а также при активной самостоятельной работе обучающихся с нормативно-правовыми актами, научной, учебной и периодической литературой по изучаемым вопросам дисциплины.

3. Требования к результатам освоения дисциплины (модуля)

Дисциплина направлена на формирование следующей компетенции в соответствии с ФГОС ВО и ОПОП ВО по специальности 38.05.01 Экономическая безопасность:

Код и наименование компетенции выпускника

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного

подхода, вырабатывать стратегию действий

Код и наименование индикатора достижения компетенций выпускника

УК-1.2. Способен находить и критически оценивать информацию для решения проблемных ситуаций, с применением современных цифровых технологий и информационных-коммуникационных средств.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

– основные понятия, угрозы и нормативно-правовую базу в области информационной безопасности экономической деятельности хозяйствующих субъектов, технологии обеспе-чения защиты корпоративной информации и управления средствами обеспечения информационной безопасности организации;

– методы поиска, сбора и обработки отечественных и зарубежных источников информации и данных для решения задач обеспечения информационной безопасности организации;

– процедуры анализа отечественных и зарубежных источников информации, данных и подготовки информационных обзоров и/или аналитических отчетов.

УМЕТЬ:

– осуществлять поиск, сбор, обработку отечественных и зарубежных источников информации и данных для целей обеспечения информационной безопасности экономической деятельности;

– анализировать отечественные и зарубежные источники информации и данные, применять методы подготовки информационных обзоров и/или аналитических отчетов.

ВЛАДЕТЬ:

– навыками поиска, сбора, обработки отечественных и зарубежных источников информации и данных для целей обеспечения информационной безопасности экономической деятельности;

– навыками анализа отечественных и зарубежных источников информации и данных, подготовки информационных обзоров и/или аналитических отчетов.

4. Содержание и структура дисциплины (модуля)

Таблица 1. Содержание дисциплины (модуля) «Информационная безопасность экономической деятельности», перечень оценочных средств и контролируемых компетенций

№ п/п	Наименование раздела/ темы	Содержание раздела	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	2	3	4	5[1]

1 В графе 5 приводятся наименования оценочных средств: защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), домашнего задания (ДЗ) написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

1	Теоретические основы информационной безопасности экономической деятельности	Основные понятия информационной безопасности. Анализ схемы взаимодействия основных субъектов и объектов обеспечения информационной безопасности. Основные понятия защиты информации. Источники данных, меры и средства обеспечения информационной безопасности.	УК-1 (УК-1.2)	Р, ДЗ, К, Т
2	Угрозы информационной безопасности экономических субъектов	Анализ и классификация угроз информационной безопасности. Анализ угроз в компьютерных сетях. Анализ угроз безопасности и уязвимости в беспроводных сетях. Анализ тенденций криминализации атак на информационные системы.	УК-1 (УК-1.2)	Р, ДЗ, К, Т
3	Нормативно-правовые основы информационной безопасности и защиты информации	Обзор нормативных правовых актов, регулирующих сферу информационной безопасности в РФ. Анализ положений ФЗ «Об информации, информационных технологиях и о защите информации». Анализ положений ФЗ «О коммерческой тайне». Анализ положений ФЗ «О персональных данных». Ответственность за нарушения в сфере компьютерной информации.	УК-1 (УК-1.2)	Р, ДЗ, Т, К
4	Политика информационной безопасности организации	Основные понятия политики информационной безопасности. Структура политики информационной безопасности организации. Базовая и специализированная политики информационной безопасности предприятия. Процедуры обеспечения	УК-1 (УК-1.2)	Р, ДЗ, К, Т

		информационной безопасности предприятия. Поиск, сбор и анализ необходимой информации для целей разработки политики информационной безопасности организации. Компоненты архитектуры безопасности корпоративной сети.		
5	Принципы многоуровневой защиты корпоративной информации	Анализ корпоративной системы с традиционной структурой. Системы «облачных» вычислений. Многоуровневый подход к обеспечению информационной безопасности корпоративной информационной системы. Подсистемы информационной безопасности традиционных корпоративных информационных систем.	УК-1 (УК-1.2)	Р, ДЗ, К, Т
6	Технологии обеспечения безопасности данных организации	Основные понятия криптографической защиты информации. Электронная цифровая подпись. Инфраструктура управления открытыми ключами PKI. Аутентификация, авторизация и администрирование действий пользователей. Анализ технологий межсетевого экранирования. Анализ технологий виртуальных защищенных сетей VNP.	УК-1 (УК-1.2)	Р, ДЗ, Т, К
7	Защита от вредоносных программ и спама	Анализ и классификация вредоносных программ. Основы работы антивирусных программ. Режимы работы антивирусных программ. Анализ возможностей «облачной» антивирусной технологии.	УК-1 (УК-1.2)	Р, ДЗ, К, Т

		Технологии защиты персональных компьютеров и корпоративных систем от действия вредоносных программ и вирусов.		
8	Управление средствами обеспечения информационной безопасности экономической деятельности	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. Анализ средств обеспечения безопасности «облачных» технологий.	УК-1 (УК-1.2)	Р, ДЗ, К, Т

Структура дисциплины (модуля) «Информационная безопасность экономической деятельности»

Таблица 2. Общая трудоемкость дисциплины составляет 3 зачетные единицы

(108 часов)

Вид работы	Трудоемкость, часов / зачетных единиц	
	VIII семестр	всего
Общая трудоемкость (в зачетных единицах)	**108**	**108**
Контактная работа (в часах):	**42**	**42**
Лекции (Л)	*28*	*28*
Практические занятия (ПЗ)	*14*	*14*
Семинарские занятия (СЗ)	*Не предусмотрены*	*Не предусмотрены*
Лабораторные работы (ЛР)	*Не предусмотрены*	*Не предусмотрены*

Самостоятельная работа (в часах):	**57**	**57**
Расчетно-графическое задание		
Реферат (Р)	6	6
Эссе (Э)	3	3
Контрольная работа (КР)	20	20
Самостоятельное изучение разделов	28	28
Курсовой проект (КП), курсовая работа (КР)	Не предусмотрена	Не предусмотрена
Подготовка и прохождение промежуточной аттестации	**9**	**9**
Вид промежуточной аттестации	**Зачет**	**Зачет**

Таблица 3. Лекционные занятия

№ п/п	Тема
1	*Теоретические основы информационной безопасности экономической деятельности. Цели и задачи темы:* изучить основные понятия, схему взаимодействия субъектов и объектов информационной безопасности; определить источники данных, 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. Цели и задачи темы:* провести обзор нормативных правовых актов, регулирующих сферу информационной безопасности в РФ; проанализировать положения основных нормативных правовых актов, регулирующих сферу информационной безопасности в РФ; определить ответственность за нарушения в сфере компьютерной информации.
4	*Политика информационной безопасности организации. Цели и задачи темы:* раскрыть основные понятия, структуру политики информационной безопасности, процедуры и компоненты архитектуры безопасности корпоративной сети; раскрыть особенности поиска, сбора и анализа необходимой информации для целей разработки политики информационной безопасности организации.
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:* провести анализ и классификацию 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 экономической деятельности. Цели и задачи темы:* раскрыть задачи управления информационной безопасностью, концепции глобального управления безопаснотью GSM; изучить процедуры аудита и мониторинга безопасности корпоративной информационной системы; провести обзор современных систем управления безопасностью корпоративных информационных систем и анализ средств обеспечения безопасности «облачных» технологий.

Таблица 4. Практические занятия (Семинарские занятия)

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

Таблица 5. Лабораторные работы – по дисциплине не предусмотрены.

Таблица 6. Самостоятельное изучение разделов дисциплины

№ п/п	Вопросы, выносимые на самостоятельное изучение
1	Источники данных, меры и средства обеспечения информационной безопасности
2	Анализ тенденций криминализации атак на информационные системы
3	Анализ положений ФЗ «Об информации, информационных технологиях и о защите информации»
4	Анализ положений ФЗ «О коммерческой тайне»
5	Анализ положений ФЗ «О персональных данных»
6	Поиск, сбор и анализ необходимой информации для целей разработки политики информационной безопасности организации
7	Компоненты архитектуры безопасности корпоративной сети
8	Многоуровневый подход к обеспечению информационной безопасности корпоративной информационной системы

9	Подсистемы информационной безопасности традиционных корпоративных информационных систем
10	Анализ технологий межсетевого экранирования
11	Анализ технологий виртуальных защищенных сетей VNP
12	Анализ возможностей «облачной» антивирусной технологии
13	Технологии защиты персональных компьютеров и корпоративных систем от действия вредоносных программ и вирусов
14	Обзор современных систем управления безопасностью корпоративных информационных систем
15	Анализ средств обеспечения 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» (контролируемая компетенция УК-1, индикатор достижения компетенции УК-1.2)

Тема №1. Теоретические основы информационной безопасности экономической деятельности

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. Опишите схему взаимодействия основных субъектов и объектов обеспечения информационной безопасности.

19. Охарактеризуйте отечественные и зарубежные источники информации и данных, необходимых для оценки информационной безопасности экономической деятельности организаций.

20. Раскройте систему мер защиты интересов субъектов информационных отношений.

21. Перечислите меры защиты информации законодательного уровня.

22. Перечислите меры защиты информации административно-организационного уровня.

23. Перечислите меры защиты информации программно-технического уровня.

24. Раскройте основные рекомендации ISTF по обеспечению информационной безопасности электронного бизнеса.

<u>Тема №2.</u> 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. Опишите суть кибероружия.

38. Охарактеризуйте современные тенденции криминализации атак на информационные ресурсы.

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

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 положений 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 положений Федерального закона «О коммерческой тайне».

12. Дайте краткую характеристику положений Федерального закона «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 организации

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 особенности поиска и сбора необходимой информации для целей разработки политики информационной безопасности организации.

27. Опишите особенности анализа необходимой информации для целей разработки политики информационной безопасности организации.

28. Опишите этапы разработки политики безопасности предприятия.

29. Опишите этап анализа рисков.

30. 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.

Тема №6. Технологии безопасности данных организации

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. Охарактеризуйте возможности «облачной» антивирусной технологии.

28. Опишите особенности работы брендмауэров.

29. Опишите средства защиты от нежелательной корреспонденции.

30. Опишите особенности работы антивирусных облаков.

31. Перечислите преимущества и недостатки антивирусных облаков.

<u>Тема №8.</u> Управление средствами обеспечения информационной безопасности экономической деятельности

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.

25. Проведите обзор современных систем управления безопасностью корпоративных информационных систем.

26. Проведите анализ средств обеспечения безопасности «облачных» технологий.

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.

Критерии оценивания при устном опросе

Баллы (оценка)	Критерии оценивания
3 балла («отлично»)	Обучающийся: – полно излагает изученный материал, дает правильное определение понятий; – обнаруживает понимание материала, может обосновать свои суждения, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; – излагает материал последовательно и правильно с точки зрения норм литературного языка.
2 балла («хорошо»)	Обучающийся: – дает ответ, удовлетворяющий тем же требованиям, установленным для оценки «отлично», но допускает не более 2 негрубых ошибок, которые сам же исправляет, и не более 3 недочетов.
1 балл («удовлетворительно»)	Обучающийся: – обнаруживает знание и понимание основных положений темы, но излагает материал неполно и допускает неточности в определении понятий (допускает более 2 негрубых ошибок); – излагает материал непоследовательно, допускает более 3 недочетов.
0 баллов («неудовлетворительно»)	Обучающийся: – обнаруживает незнание большей части соответствующего раздела изучаемого материала (допускает грубые ошибки).

Грубые ошибки: неправильный ответ или пояснения к ответу на поставленный вопрос;

неправильное определение базовых терминов по дисциплине.

Негрубые ошибки: неточный или неполный ответ на поставленный вопрос; при правильном ответе неумение самостоятельно или полно обосновать и проиллюстрировать его.

Недочеты: непоследовательность, неточность в языковом оформлении излагаемого.

Баллы (1-3) могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов обучающегося на протяжении занятия.

5.1.2. Оценочные материалы для выполнения рефератов по дисциплине «Информационная безопасность экономической деятельности»

(контролируемая компетенция УК-1, индикатор достижения компетенции УК-1.2)

Тема №1. Теоретические основы информационной безопасности экономической деятельности

1. Анализ основных понятий и терминов в области информационной безопасности экономической деятельности.

2. Обеспечение информационной безопасности в свете проблем современной экономической системы.

3. Понятие и виды информации как объекта права собственности. Объект защиты информации.

4. Обзор источников информации и данных для целей обеспечения информационной безопасности экономической деятельности.

5. Анализ проблем развития теории и практики обеспечения информационной безопасности предприятия.

6. Оценка основных составляющих информационной безопасности и их значения для субъектов экономических отношений.

Тема №2. Угрозы информационной безопасности экономических субъектов

1. Модель гипотетического нарушителя информационной безопасности экономических субъектов.

2. Случайные и преднамеренные угрозы информационной безопасности экономических субъектов.

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

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 организации

1. Разработка разделов «Цель» и «Область действия» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

2. Разработка раздела «Объект защиты» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

3. Разработка раздела «Безопасность персонала» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

4. Разработка раздела «Контроль доступа» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

5. Разработка раздела «Политика допустимого использования информационных ресурсов» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

6. Разработка раздела «Приобретение, разработка и обслуживание информационных систем» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

7. Разработка раздела «Аудит информационной безопасности» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

8. Разработка раздела «Система управления информационной безопасностью» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

9. Разработка раздела «Оценка и обработка рисков» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

10. Разработка раздела «Физическая безопасность» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

11. Разработка раздела «Управление инцидентами информационной безопасности» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

12. Разработка раздела «Ответственность» Политики информационной безопасности организации: особенности поиска, сбора и анализа информации.

Тема №5. Принципы многоуровневой защиты корпоративной информации

1. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн).

2. Особенности защиты информации, составляющей коммерческую тайну компании.

3. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры.

4. Минимизация ущерба от аварий и стихийных бедствий. Дублирование информации.

5. Повышение надежности информационной системы. Создание отказоустойчивых информационных систем.

6. Оптимизация взаимодействия пользователей информационной системы предприятия и обслуживающего ее персонала.

Тема №6. Технологии безопасности данных организации

1. Криптографические методы защиты информации.

2. Современные симметричные и асимметричные криптографические системы.

3. Оценка криптостойкости шифров. Правила работы с паролями.

4. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.

5. Методики обоснования выбора средств технической и криптографической защиты информации.
6. 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 экономической деятельности

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.

Требования к структуре, содержанию, методические рекомендации по написанию реферата

В соответствии с Положением о рабочей программе дисциплины (модуля) по образовательным программам высшего образования в КБГУ, принятого УМС КБГУ 01 июня 2018 г. (протокол № 8) и утвержденного проректором по УР (https://kbsu.ru/wp-content/uploads/2018/12/rpd01.pdf) *реферат* – доклад на определенную тему, включающий обзор соответствующих литературных и других источников; краткое изложение содержания научной работы, книги (или ее части), статьи с основными фактическими сведениями и выводами. Реферат является творческой исследовательской работой, основанной, прежде всего, на изучении значительного количества научной и иной литературы по теме исследования.

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

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. Рекомендуется использовать при подготовке реферата не менее 5 источников.

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. –

Критерии оценивания при защите реферата

Баллы (оценка)	Критерии оценивания
3 балла («отлично»)	– соответствие содержания заявленной теме, отсутствие в тексте отступлений от темы работы; – логичность и последовательность в изложении материала в работе; – качество работы с зарубежными и отечественными источниками информации и данных, Интернет-ресурсами (актуальность источников, достаточность использованных источников для раскрытия темы работы); – правильность оформления работы (соответствие стандарту в представлении текста, ссылок, цитат, таблицы, графического материала и т.д.); – способность к анализу и обобщению информационного материала, степень полноты обзора состояния вопроса, обоснованность выводов в работе; – работа представлена в срок; – способность к публичной коммуникации, получены обоснованные ответы на дополнительные вопросы аудитории и преподавателя при защите работы.
2 балла («хорошо»)	– соответствие содержания заявленной теме, незначительные отступления в

	тексте от темы работы; – незначительные нарушения в логичности и последовательности изложения материала в работе; – в целом достаточность и актуальность использованных зарубежных и отечественных источников информации и данных, Интернет-ресурсов для раскрытия темы реферата; – выполнены основные требования к оформлению работы (незначительные неточности и отступления от стандарта в представлении текста, ссылок, цитат, таблицы, графического материала и т.д.); – достаточный уровень проявленной способности к анализу и обобщению информационного материала, достаточная степень полноты обзора состояния вопроса и обоснованности выводов в работе; – работа представлена в срок, но с некоторыми недоработками; – неполные ответы (незначительные ошибки) на дополнительные вопросы аудитории и преподавателя при защите работы.
1 балл («удовлетворительно»)	– имеются существенные отступления содержания от заявленной темы, значительные отступления в тексте от темы работы; – значительные нарушения в логичности и последовательности изложения материала в работе; – в целом недостаточность, неполная актуальность использованных зарубежных и отечественных источников информации и данных, Интернет-ресурсов для раскрытия темы реферата; – не выполнены основные требования к оформлению работы (значительные неточности и отступления от стандарта в представлении текста, ссылок, цитат, таблицы, графического материала и т.д.); – недостаточный уровень проявленной способности к анализу и обобщению информационного материала, тема освещена частично, отсутствуют выводы в работе; – работа представлена со значительным опозданием (более 1 недели), отсутствуют отдельные фрагменты работы; – неполные ответы со значительными ошибками на дополнительные вопросы аудитории и преподавателя при защите работы.
0 баллов («неудовлетворительно»)	– тема работы не раскрыта, обнаруживается существенное непонимание ее содержания; – поставленные задачи не выполнены или выполнены их отдельные несущественные части; – работа не представлена.

5.1.3. Оценочные материалы для контрольной работы по дисциплине «Информационная

безопасность экономической деятельности (контролируемая компетенция УК-1, индикатор достижения компетенции УК-1.2)

Контрольная работа № 1

Цели контрольной работы: закрепление теоретического материала, развитие практических навыков определения источников информации, мер и средств обеспечения информационной безопасности экономической деятельности (контролируемая компетенция: УК-1.2)

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

Задание 1. Решите тестовое задание.

1. 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

2. Ущерб полного или частичного разрушения информации – это

a) стоимость утраты

b) стоимость скрытого нарушения целостности

c) стоимость потери конфиденциальности

d) нет верного ответа

3. 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.)

4. Не является преднамеренным воздействием на информационную систему

a) подбор пароля

b) хищение информации

c) перехват информации

d) модификация информации

5. 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

6. 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

7. 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

8. Результатом реализации угрозы перехвата может стать

a) нарушение доступности данных

b) отказ в обслуживании

c) нарушение конфиденциальности данных

d) изменение конфигурации периферийных устройств

9. 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

10. Уголовно наказуемые общественно опасные действия, в которых машинная информация является объектом посягательства – это

a) компьютерное преступление

b) несанкционированное действие

c) компьютерное мошенничество

d) кража

Задание 2. 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.
Г. 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			
9	Производственный процесс			
10	Отправление товара с курьером			

<u>Контрольная работа № 2</u>

Цели контрольной работы: закрепление теоретического материала, развитие практических навыков определения угроз информационной безопасности экономической деятельности (контролируемая компетенция: УК-1.2)

Задачи контрольной работы: раскрыть содержание, виды угроз информационной безопасности организации.

Задание 1. Решите тестовое задание.

1. 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

2. 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

3. Основными направлениями защиты информации являются

a) предупреждение угроз

b) выявление угроз

c) ликвидация угроз

d) ликвидация последствий угроз

e) стабилизация угроз

f) регистрация угроз

4. Действия, направленные на устранение действующей угрозы и конкретных преступных действий – это

a) предупреждение угроз

b) выявление угроз

c) обнаружение угроз

d) ликвидация угроз

5. 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

6. 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

7. 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

8. 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

9. Результатом реализации угрозы перехвата может стать

a) нарушение доступности данных

b) отказ в обслуживании

c) нарушение конфиденциальности данных

d) изменение конфигурации периферийных устройств

10. 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

Задание 2. Содержание задания: проведите классификацию следующих реальных ситуаций как угроз информационной безопасности экономической деятельности.

А. По природе их возникновения.

Б. По степени преднамеренности их возникновения.

В. По источнику их возникновения.

Г. По положению источника их возникновения.

Д. По степени их зависимости от активности информационной системы.

Е. По степени их воздействия на информационную систему.

Ж. По способу доступа к ресурсам информационной системы.

З. По текущему месту расположения информации, хранимой и обрабатываемой в информационной системе.

Ситуация 1. Сбой сетевого оборудования.

Ситуация 2. Ошибка персонала технической поддержки.

Ситуация 3. Нелегальное использование программного обеспечения.

Ситуация 4. Взрыв на предприятии, приведший к уничтожению его информационной системы.

Ситуация 5. «Маскарад» (присвоение идентификатора пользователя).

Ситуация 6. Акустическая разведка.

Ситуация 7. Кража бумажных документов инсайдерами

Ситуация 8. Утечка конфиденциально информации по сетевым каналам связи.

Ситуация 9. Неумышленное раскрытие информации сотрудником компании.

Ситуация 10. Заражение компьютерным вирусом.

Контрольная работа № 3

Цели контрольной работы: закрепление теоретического материала, развитие практических навыков анализа нормативно-правовой базы в сфере информационной безопасности и защиты информации (контролируемая компетенция: УК-1.2)

Задачи контрольной работы: провести анализ уголовной ответственности за преступления в сфере компьютерной информации, административной ответственности в области связи, в соответствии с действующим законодательством РФ.

Задание 1. Решите тестовое задание.

1.Основополагающими документами по информационной безопасности в РФ являются

a) Конституция РФ

b) Концепция национальной безопасности

c) Уголовный кодекс РФ

d) Закон об информационной безопасности

2. 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

3. 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

4. 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

5. Информация, с помощью которой можно однозначно идентифицировать физическое лицо – это

a) конфиденциальная информация

b) персональные данные

c) государственная тайна

d) служебная тайна

6. 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

e) Конституция РФ

f) Концепция национальной безопасности

g) Уголовный кодекс РФ

h) Закон об информационной безопасности

7. Документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности – это

e) конфиденциальная информация

f) персональные данные

g) государственная тайна

h) служебная тайна

8. Хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей – это

a) компьютерное преступление

b) несанкционированное действие

c) мошенничество в сфере компьютерной информации

d) кража в сфере компьютерной информации

9. Интернет-мошенничество, целью которого является получение доступа к конфиденциальным данным пользователей (логинам, паролям) – это

a) фишинг

b) кардинг

c) фарминг

d) скимминг

10. Уголовно наказуемые общественно опасные действия, в которых машинная информация является объектом посягательства – это

e) компьютерное преступление

f) несанкционированное действие

g) компьютерное мошенничество

h) кража

Задание 2. Оформите отдельно для каждого вида преступления в сфере компьютерной информации его характеристику и меры наказания, в соответствии с УК РФ.

Преступление в сфере компьютерной безопасности	Статья УК РФ	Характеристика преступления	Уголовная ответственность
Создание, использование и распространение вредоносных			

компьютерных программ			
Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации			
Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей			
Неправомерный доступ к компьютерной информации			

Задание 3. Оформите отдельно для каждого вида административного правонарушения в области связи и информации его характеристику и меры наказания, в соответствии с Кодексом РФ об административных правонарушениях.

Преступление в сфере компьютерной безопасности	Статья КоАП РФ	Характеристика правонарушения	Административная ответственность
Использование средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия установленным требованиям			
Разглашение информации с ограниченным доступом			
Нарушение законодательства Российской Федерации в области персональных данных			
Нарушение правил защиты информации			
Незаконная деятельность в области защиты информации			

Контрольная работа № 4

Цели контрольной работы: закрепление теоретического материала, развитие практических навыков разработки политики информационной безопасности экономического субъекта (контролируемая компетенция: УК-1.2)

Задачи контрольной работы: провести анализ потенциальных и реальных угроз экономического

субъекта и на его основе актуализировать политику его информационной безопасности.

Задание 1. Решите тестовое задание.

1. В политике безопасности предприятия не рассматривается

a) требуемый уровень защиты данных

b) анализ рисков

c) защищенность сотрудников

d) роли субъектов информационных отношений

2. 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

3. Стратегия организации в области информационной безопасности, мера внимания и количество ресурсов, которые руководство компании считает целесообразным выделить для обеспечения информационной безопасности – это

e) политика безопасности

f) стратегия безопасности

g) концепция безопасности

h) нет верного ответа

4. Политика безопасности разрабатывается на уровне обеспечения информационной безопасности

a) Информационном

b) Административном

c) Законодательно-правовом

d) Программно-техническом

5. 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

6. Основные уровни обеспечения защиты информации

a) законодательный
b) физический
c) административный
d) процедурный
e) программно-технический
f) вероятностный
g) распределительный

7. Стратегия организации в области информационной безопасности, мера внимания и количество ресурсов, которые руководство компании считает целесообразным выделить для обеспечения информационной безопасности – это

h) политика безопасности
i) стратегия безопасности
j) концепция безопасности
k) нет верного ответа

8. 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

9. Этот уровень не относится к уровням обеспечения информационной безопасности

a) информационный

b) административный

c) законодательно-правовой

d) программно-технический

10. Физические средства защиты информации

a) средства, которые реализуются в виде автономных устройств и систем
b) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
c) это программы, предназначенные для выполнения функций, связанных с защитой информации
d) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Задание 2. Выполните практическое задание.

Вы возглавляете Департамент информационной безопасности коммерческого банка. Руководство банка поставило вам следующую задачу – актуализировать (привести в соответствие с требованиями действующего законодательства и современными угрозами информационной безопасности кредитной организации) Политику информационной безопасности банка.

1. Опишите последовательность Ваших действий для решения поставленной задачи.

2. Опишите структуру базовой Политики информационной безопасности, которую Вы считаете рациональной и логичной.
3. Охарактеризуйте, какие специализированные Политики информационной безопасности необходимо разработать для обеспечения информационной защиты банка.
4. Опишите, какие существуют потенциальные и реальные угрозы информационной безопасности банка.
5. Предложите свой вариант защиты банка от данных потенциальных и реальных угроз.
6. Составьте аналитический отчет, в котором обоснуйте программу актуализации информационной политики коммерческого банка.

Задание 3. Выполните практическое задание.

Вы возглавляете Департамент информационной безопасности крупного сетевого онлайн-ритейлера. Руководство банка поставило вам следующую задачу – актуализировать (привести в соответствие с требованиями действующего законодательства и современными угрозами информационной безопасности кредитной организации) Политику информационной безопасности компании.

1. Опишите последовательность Ваших действий для решения поставленной задачи.
2. Опишите структуру базовой Политики информационной безопасности, которую Вы считаете рациональной и логичной.
3. Охарактеризуйте, какие специализированные Политики информационной безопасности необходимо разработать для обеспечения информационной защиты компании.
4. Опишите, какие существуют потенциальные и реальные угрозы информационной безопасности компании.
5. Предложите свой вариант защиты компании от данных потенциальных и реальных угроз.
6. Составьте аналитический отчет, в котором обоснуйте программу актуализации информационной политики компании.

<u>Контрольная работа № 5</u>

Цели контрольной работы: закрепление теоретического материала, развитие практических навыков оценки современного антивирусного программного обеспечения (контролируемая компетенция: УК-1.2)

Задачи контрольной работы: определить основные функции, достоинства и недостатки современного антивирусного программного обеспечения.

Задание 1. Решите тестовое задание.

1. Технические средства защиты информации

a) средства, которые реализуются в виде автономных устройств и систем
b) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
c) это программы, предназначенные для выполнения функций, связанных с защитой информации
d) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

2. Атаки, которые предпринимают хакеры на программном уровне

a) атаки на уровне ОС

b) атаки на уровне сетевого ПО
c) атаки на уровне пакетов прикладных программ
d) атаки на уровне СУБД

3. В зависимости от деструктивных возможностей компьютерные вирусы бывают

a) сетевые, файловые, загрузочные, комбинированные
b) безвредные, неопасные, опасные, очень опасные
c) резидентные, нерезидентные
d) полиморфные, макровирусы, вирусы-невидимки, «паразитические», «студенческие», «черви», компаньон-вирусы

4. 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

5. Жизненный цикл вируса состоит из этапов

a) внедрение (инфицирование)

b) инкубационный период

c) выполнение специальных функций

d) саморазмножение (репродуцирование)

e) проявление

6. Способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то

a) «За дураком»

b) «Брешь»

c) «Компьютерный абордаж»

d) «За хвост»

e) «Неспешный выбор»

7. Способ несанкционированного доступа к информации, который заключается в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме

a) «За дураком»

b) «Брешь»

c) «Компьютерный абордаж»

d) «За хвост»

e) «Неспешный выбор»

8. Способ несанкционированного доступа к информации, который заключается в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе

a) «За дураком»

b) «Брешь»

c) «Компьютерный абордаж»

d) «За хвост»

e) «Неспешный выбор»

9. 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

10. 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

Задание 2. 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.
Г. 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			

Контрольная работа № 6

Цели контрольной работы: закрепление теоретического материала, развитие практических навыков оценки экономических параметров для обоснования мероприятий информационной безопасности по снижению IT-рисков (контролируемая компетенция: УК-1.2)

Задачи контрольной работы: провести расчеты и составить аналитический отчет по экономической целесообразности включения мероприятий безопасности в План снижения IT-рисков.

Задание 1. Решите тестовое задание.

1. К видам защиты информации относятся

a) правовые и законодательные
b) морально-этические
c) юридические

2. 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

3. Типы межсетевых экранов

a) межсетевые экраны прикладного уровня

b) гибридные межсетевые экраны

c) межсетевые экраны с пакетной фильтрацией

d) релевантные межсетевые экраны

4. Ключевые компоненты виртуальной сети VNP

a) сервер VNP

b) алгоритмы шифрования

c) система аутентификации

d) система документирования

e) протокол VNP

5. 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

6. 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

7. Основные типы систем предотвращения атак – IDS

a) узловые

b) сетевые

c) протокольные

d) все перечисленные

8. Несанкционированный доступ (НСД)

a) доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
b) создание резервных копий в организации

c) правила и положения, выработанные в организации для обхода парольной защиты
d) вход в систему без согласования с руководителем организации
e) удаление не нужной информации

9. К методам защиты от НСД относятся

a) разделение доступа
b) разграничение доступа
c) увеличение доступа
d) ограничение доступа
e) аутентификация и идентификация

10. Укажите соответствие для всех 4 вариантов ответа
1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей
4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

a) защита информации от утечки по акустическому каналу
b) защита информации от утечки по визуально-оптическому каналу
c) защита информации от утечки по электромагнитным каналам
d) защита информации от утечки по материально-вещественному каналу

Задание 2. Работа в малых группах. Выполните следующее практическое задание.

Описание ситуации

Ваша организация недавно приобрела новый актив – компанию, предоставляющую транспортные услуги. Организация имеет намерение провести реорганизацию своего нового бизнеса, поднять уровень IT, добиться надежного уровня защищенности информационных активов, после чего продать этот бизнес ориентировочно не менее чем через 5 лет. Поэтому принято решение не распространять на вновь приобретенную компанию Политику, стандарты информационной безопасности и прочие организационно-административные документы организации, а провести независимую оценку состояния информационной безопасности (ИБ), оценить стоимость необходимых мероприятий ИБ и после этого вернуться к решению вопроса о дальнейших действиях в отношении приобретенного бизнеса.

По результатам анализа информационных рисков консультанты разработали План мероприятий по снижению IT-рисков. Представленный План вызвал серьезную озабоченность руководства организации размером запрашиваемой суммы на его реализацию. Вам дано поручение подготовить экономическое обоснование запрашиваемых средств.

Содержание задания

1. Рассчитать экономические показатели экономической целесообразности включения мероприятий безопасности, используя данные, приведенные в Плане мероприятий по ИБ, исходя из того, что: расчетный период равен 3-м годам; остаточные риски и некоторые другие данные по реализуемым мероприятиям ИБ представлены в нижеприведенной таблице.

2. Составьте аналитический отчет с содержательной интерпретацией полученных результатов, который будете использовать для убеждения руководства в обоснованности затрат на обеспечение ИБ.

3. Если, по вашему мнению, есть другие экономические показатели, которые можно использовать для обоснования затрат па реализацию Плана, приведите их.

Мероприятия	Риски (в монетарном исчислении), тыс. руб.	Стоимость мероприятия, тыс. руб.	Стоимость технической поддержки	Зарплата обслуживающего персонала в год, тыс. руб.	Величина остаточного риска, тыс. руб.
Разработка политики стандартов безопасности	600000	340000	34000	0	600
Усиление антивирусной защиты	600000	200000	30000	22000	2000
Шифрование почтовых сообщений	2000000	220000	34000	7000	20000
Выявление и блокировка взломщиков, борьба с похищением данных	200000	400000	40000	34000	2000

Методические рекомендации для выполнения контрольной работы

Контрольная работа – одна из форм проверки и оценки усвоения знаний. По результатам контрольной работы можно судить об уровне самостоятельности и активности обучающегося в учебном процессе. Контрольная работа реализуется в виде аудиторной работы.

Основные задачи контрольной работы:

1) закрепление полученных ранее теоретических знаний;

2) выработка навыков самостоятельной научно-исследовательской работы;

3) выяснение подготовленности студентов к будущей практической работе;

4) выявление способностей к научно-исследовательской и поисковой деятельности.

Выполнение контрольных работ необходимо для более полного освоения дисциплины и играет существенную роль в формировании профессиональных компетенций.

При подготовке к контрольной работе необходимо придерживаться следующей технологии:

1. Внимательно изучить лекционный материал по теме контрольной работы.

2. Найти и проработать соответствующие разделы в рекомендованных нормативных документах, учебниках и дополнительной литературе.

Критерии оценивания контрольных работ

Баллы (оценка)	Критерии оценивания
4 балла («отлично»)	– обучающийся выполнил работу полностью, без ошибок и недочетов
3 балла («хорошо»)	– обучающийся в целом выполнил задание (более 2/3 работы), допускается наличие не более одной негрубой ошибки и одного недочета, не более трех недочетов
1-2 балла («удовлетворительно»)	– задание выполнено не полностью (более 1/2, но менее 2/3 работы), допущены: не более одной грубой ошибки и двух недочетов; не более одной грубой и одной негрубой ошибки; не более трех негрубых ошибок и одного недочета
0 баллов («неудовлетворительно»)	– задание выполнено не полностью (менее 1/2 работы), число ошибок и недочетов превысило норму, установленную для оценки «удовлетворительно»

Грубые ошибки:

– незнание или неправильное применение правил, алгоритмов, существующих зависимостей, лежащих в основе выполнения задания или используемых в ходе его выполнения;

– неправильный выбор действий, операций, методов;

– неумение делать выводы и обобщения, что определяет несоответствие аналитического заключения (отчета) выполненным действиям и полученным результатам.

Негрубые ошибки:

– нерациональный выбор действий, операций, методов;

– ошибки при выполнении расчетных действий, не повлекшие ложность выводов в аналитическом заключении (отчете).

Недочеты:

– небрежное оформление записей и расчетов;

– нарушение логики построения аналитического заключения (отчета).

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. На рубежные контрольные мероприятия рекомендуется выносить весь программный материал (все разделы) по дисциплине.

5.2.1. Оценочные материалы для коллоквиума по дисциплине «Информационная безопасность

<u>экономической деятельности» (контролируемая компетенция УК-1, индикатор достижения компетенции УК-1.2)</u>

Рубежный контроль № 1

1. Основные понятия информационной безопасности.

2. Анализ схемы взаимодействия основных субъектов и объектов обеспечения информационной безопасности.

3. Основные понятия защиты информации.

4. Источники данных, меры и средства обеспечения информационной безопасности.

5. Анализ и классификация угроз информационной безопасности.

6. Анализ угроз в компьютерных сетях.

7. Анализ угроз безопасности и уязвимости в беспроводных сетях.

8. Анализ тенденций криминализации атак на информационные системы.

9. Обзор нормативных правовых актов, регулирующих сферу информационной безопасности в РФ.

10. Анализ положений ФЗ «Об информации, информационных технологиях и о защите информации».

11. Анализ положений ФЗ «О коммерческой тайне».

12. Анализ положений ФЗ «О персональных данных».

13. Ответственность за нарушения в сфере компьютерной информации.

Рубежный контроль № 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. Поиск, сбор и анализ необходимой информации для целей разработки политики информационной безопасности организации.

6. Компоненты архитектуры безопасности корпоративной сети.

7. Анализ корпоративной системы 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. Анализ технологий межсетевого экранирования.

16. Анализ технологий виртуальных защищенных сетей VNP.

Рубежный контроль № 3

1. Анализ и классификация вредоносных программ.

2. Основы работы антивирусных программ.

3. Режимы работы антивирусных программ.

4. Анализ возможностей «облачной» антивирусной технологии.

5. Технологии защиты 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. Анализ средств обеспечения безопасности «облачных» технологий.

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.

Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума. Методические указания состоят из рекомендаций по изучению источников и литературы, вопросов для самопроверки и кратких конспектов ответа, относящихся к пунктам плана каждой темы. Это должно помочь обучающимся целенаправленно организовать работу по овладению материалом и его запоминанию. 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.

Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым обучающимся или беседы в небольших группах (2-3 человека). Обычно преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, проверяет конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания.

Критерии оценивания при коллоквиуме

Баллы (оценка)	Критерии оценивания
5-6 баллов («отлично»)	Ответы получены 80-100% заданных вопросов. Обучающийся: – полно излагает изученный материал, дает правильное определение понятий; – обнаруживает понимание материала, может обосновать свои суждения, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; – излагает материал последовательно и правильно с точки зрения норм литературного языка.
3-4 балла («хорошо»)	Ответы даны на 60-80% заданных вопросов. Обучающийся: – дает ответ, удовлетворяющий тем же требованиям, установленным для оценки «отлично», но допускает не более 2 негрубых ошибок, которые сам же исправляет, и не более 2 недочетов.
1-2 балл («удовлетворительно»)	Ответы даны на 40-60% вопросов. Обучающийся: – обнаруживает знание и понимание основных положений темы, но излагает материал неполно и допускает неточности в определении понятий (допускает более 2 негрубых ошибок); – излагает материал непоследовательно, допускает более 2 недочетов.
0 баллов («неудовлетворительно»)	Ответы даны менее чем на 40% вопросов. Обучающийся: – обнаруживает незнание большей части соответствующего раздела изучаемого материала (допускает грубые ошибки).

Грубые ошибки: неправильный ответ или пояснения к ответу на поставленный вопрос; неправильное определение базовых терминов по дисциплине.

Негрубые ошибки: неточный или неполный ответ на поставленный вопрос; при правильном ответе неумение самостоятельно или полно обосновать и проиллюстрировать его.

Недочеты: непоследовательность, неточность в языковом оформлении излагаемого.

5.2.2. Оценочные материалы для проведения тестирования (образцы тестовых заданий) по дисциплине «Информационная безопасность экономической деятельности» (контролируемая

компетенция УК-1, индикатор достижения компетенции УК-1.2)

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

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

e) Информационная безопасность

f) Компьютерная безопасность

g) Защита информации

h) 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

e) Информационная безопасность

f) Компьютерная безопасность

g) Защита информации

h) 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. Категориями ценности информации с точки зрения информационной безопасности являются

a) Конфиденциальность

b) Целостность

c) Статичность

d) Аутентичность

e) Адекватность

f) Доступность

g) Аппелируемость

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

a) Аутентичность

b) Аппелируемость

c) Достоверность

d) Статичность

17. Аутентичность предполагает

a) Проверку прав доступа

b) Доказательство авторства документа

c) Изменение авторства документа

d) Контроль целостности данных

18. 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

19. 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

20. Не является преднамеренным воздействием на информационную систему

a) Подбор пароля

b) Хищение информации

c) Перехват информации

d) Модификация информации

21. 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

22. 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

23. 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

24. Результатом реализации угрозы перехвата может стать

a) Нарушение доступности данных

b) Отказ в обслуживании

c) Нарушение конфиденциальности данных

d) Изменение конфигурации периферийных устройств

25. 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

26. 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

27. Методы организации разграничения доступа к информации в информационных системах

a) Матричный

b) Реляционный

c) Полномочный (мандатный)

28. Способы преобразования при шифровании

1. Подстановка

2. Перестановка

3. Аналитическое преобразование

4. Кодирование

5. Гаммирование

29. В криптосистему не входит

a) Алгоритм шифрования

b) Полиморфик-генератор

c) Система управления ключами

d) Нет верного ответа

30. При асимметричном шифровании для шифрования и расшифровки используются

a) Два взаимосвязанных ключа

b) Один открытый ключ

c) Два открытых ключа

d) Один закрытый ключ

31. Цифровая подпись не обеспечивает

a) Контроль целостности документа

b) Конфиденциальность документа

c) Доказательное подтверждение авторства документа

d) Восстановление поврежденного документа

32. Программные модули или аппаратные устройства, регистрирующие каждое нажатие клавиши на клавиатуре компьютера

a) Скриншоты

b) Кайлотеры

c) Брандмауэры

d) Браузеры

33. Размер ключа в ГОСТ 28147-89

a) 128 бит

b) 56 бит

c) 64 бит

d) 256 бит

34. Активный перехват информации - это перехват, который

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций

c) неправомерно использует технологические отходы информационного процесса

d) осуществляется путем использования оптической техники

e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера

35. Пассивный перехват информации - это перехват, который

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций

c) неправомерно использует технологические отходы информационного процесса

d) осуществляется путем использования оптической техники

e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера

36. Аудиоперехват перехват информации - это перехват, который

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций

c) неправомерно использует технологические отходы информационного процесса

d) осуществляется путем использования оптической техники

e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера

37. Просмотр мусора - это перехват информации, который

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций

c) неправомерно использует технологические отходы информационного процесса

d) осуществляется путем использования оптической техники

e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера

38. Хакер – это

a) лицо, которое взламывает интрасеть в познавательных целях

b) мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных

c) лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО

d) мошенник, который обманным путем выманивает у доверчивых пользователей сети конфиденциальную информацию

39. Фракер – это

a) лицо, которое взламывает интрасеть в познавательных целях

b) мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных

c) лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО

d) мошенник, который обманным путем выманивает у доверчивых пользователей сети конфиденциальную информацию

40. Фишер – это

a) лицо, которое взламывает интрасеть в познавательных целях

b) мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных

c) лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО

d) мошенник, который обманным путем выманивает у доверчивых пользователей сети конфиденциальную информацию

Методические рекомендации к тестированию

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

При самостоятельной подготовке к тестированию обучающемуся 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.

Критерии оценивания по тестовым заданиям

Предел длительности контроля	30 мин
Предлагаемое количество заданий из одного контролируемого подраздела	30 тестовых заданий
Критерии оценки	% верно выполненных тестовых заданий
«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 «Информационная безопасность экономической деятельности» является оценка качества ее освоения обучающимися.

Промежуточная аттестация предназначена для объективного подтверждения и оценивания достигнутых результатов обучения после завершения изучения дисциплины. Осуществляется в конце 8 семестра и представляет собой итоговую оценку знаний по дисциплине «Информационная безопасность экономической деятельности» в виде проведения зачета.

Промежуточная аттестация по дисциплине «Информационная безопасность экономической деятельности» проводится в письменной форме. На промежуточную аттестацию отводится от 15 до 30 баллов.

5.3.1. Вопросы к зачету (контролируемая компетенция УК-1, индикатор достижения компетенции УК-1.2)

Основные понятия информационной безопасности

1. Анализ схемы взаимодействия основных субъектов и объектов обеспечения информационной безопасности.
2. Основные понятия защиты информации.
3. Источники данных, меры и средства обеспечения информационной безопасности.
4. Анализ и классификация угроз информационной безопасности.
5. Анализ угроз в компьютерных сетях.
6. Анализ угроз безопасности и уязвимости в беспроводных сетях.
7. Анализ тенденций криминализации атак на информационные системы.
8. Обзор нормативных правовых актов, регулирующих сферу информационной безопасности в РФ.
9. Анализ положений ФЗ «Об информации, информационных технологиях и о защите информации».

10. Анализ положений ФЗ «О коммерческой тайне».

11. Анализ положений ФЗ «О персональных данных».

12. Ответственность за нарушения в сфере компьютерной информации.

13. Основные понятия политики информационной безопасности.

14. Структура политики информационной безопасности организации.

15. Базовая и специализированная политики информационной безопасности предприятия.

16. Процедуры обеспечения информационной безопасности предприятия.

17. Поиск, сбор и анализ необходимой информации для целей разработки политики информационной безопасности организации.

18. Компоненты архитектуры безопасности корпоративной сети.

19. Анализ корпоративной системы с традиционной структурой.

20. Системы «облачных» вычислений.

21. Многоуровневый подход к обеспечению информационной безопасности корпоративной информационной системы.

22. Подсистемы информационной безопасности традиционных корпоративных информационных систем.

23. Основные понятия криптографической защиты информации.

24. Электронная цифровая подпись.

25. Инфраструктура управления открытыми ключами PKI.

26. Аутентификация, авторизация и администрирование действий пользователей.

27. Анализ технологий межсетевого экранирования.

28. Анализ технологий виртуальных защищенных сетей VNP.

29. Анализ и классификация вредоносных программ.

30. Основы работы антивирусных программ.

31. Режимы работы антивирусных программ.

32. Анализ возможностей «облачной» антивирусной технологии.

33. Технологии защиты персональных компьютеров и корпоративных систем от действия вредоносных программ и вирусов.

34. Задачи управления информационной безопасностью.

35. Концепция глобального управления безопаснотью GSM.

36. Функционирование системы управления информационной безопасностью корпоративной информационной системы.

37. Аудит безопасности корпоративной информационной системы.

38. Мониторинг безопасности информационной системы компании.

39. Обзор современных систем управления безопасностью корпоративных информационных систем.

40. Анализ средств обеспечения безопасности «облачных» технологий.

Методические рекомендации по подготовке и процедуре осуществления контроля выполнения

Подготовка к экзамену производится последовательно и планомерно. Определяется место каждого экзаменационного вопроса в соответствующем разделе темы. Изучаются лекционные материалы и соответствующие разделы рекомендованных источников основной и дополнительной литературы. При этом полезно делать краткие выписки и заметки.

Для обеспечения полноты ответа на экзаменационные вопросы и лучшего запоминания теоретического материала рекомендуется составлять план ответа на каждый вопрос. Это позволит сэкономить время для подготовки непосредственно перед экзаменом за счет обращения не к литературе, а к своим записям.

При подготовке необходимо выявлять наиболее сложные вопросы, с тем, чтобы обсудить их с преподавателем на консультациях. Нельзя ограничивать подготовку к экзамену простым повторением изученного материала. Необходимо углубить и расширить ранее приобретенные знания за счет новых идей и положений.

5.3.2. Примеры типовых контрольных заданий на экзамене (контролируемая компетенция УК-1, индикатор достижения компетенции УК-1.2)

Цель контрольных заданий: закрепление теоретических знаний и развитие практических навыков анализа угроз и показателей информационной безопасности экономической деятельности, подготовки аналитических отчетов.

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.

А. Установите (в соответствии с действующим законодательством), кто будет отвечать за случившуюся аварию.

Б. Определите, какой будет его ответственность.

В. 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).

А. Оцените ситуацию, определите виновных и причины.

Б. Разработайте меры по предотвращению подобных ситуаций.

В. 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.

В. 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.

КОНТРОЛЬНОЕ ЗАДАНИЕ 6.

Молодой человек из Владивостока приобрел фишинговую программу и путем подбора логина и

пароля внедрялся в информационные системы компаний. Чтобы анонимно выходить в Интернет, мошенник использовал программу для сокрытия IP-адреса. Жертвами мошенника стали 18 автомагазинов. Получив доступ к электронной почте менеджеров, хакер вступал в переписку с клиентами от лица автомагазина. Он предлагал приобрести автокомплектующие на условиях полной оплаты на его банковскую карту. После перечисления денег мошенник удалял переписку из почты компании и переставал выходить на связь с клиентом. За пять месяцев преступнику удалось заработать 1 млн руб.

А. Оцените ситуацию, определите причины, позволившие мошеннику совершить данное преступление.

Б. Разработайте меры по предотвращению подобных ситуаций.

В. Составьте аналитический отчет.

Методические рекомендации по подготовке и процедуре осуществления контроля выполнения

При подготовке к выполнению контрольных заданий необходимо воспользоваться лекционным материалом, а также повторить алгоритм решения подобных задач, решенных на практических занятиях.

Критерии оценивания

Максимальная сумма баллов, набираемая обучающимся по дисциплине, включает две составляющие:

– *первая составляющая* – оценка регулярности, своевременности и качества выполнения обучающимся учебной работы по изучению дисциплины в течение периода изучения дисциплины (сумма – не более 70 баллов). Баллы, характеризующие успеваемость обучающегося по дисциплине, набираются им в течение всего периода обучения за изучение отдельных тем и выполнение отдельных видов работ. Общий балл складывается в результате проведения текущего и рубежного контроля по дисциплине:

Шкала оценивания			
0-35 баллов	36-50 баллов	51-60 баллов	61-70 баллов
Частичное посещение аудиторных занятий. Неудовлетворительное выполнение заданий на практических (семинарских) занятиях. Плохая подготовка к БРМ. Обучающийся не допускается к промежуточной аттестации	Полное или частичное посещение аудиторных занятий. Частичное выполнение и защита заданий на практических (семинарских) занятиях. Выполнение тестовых заданий, ответы на коллоквиуме на оценки «удовлетворительно»	Полное или частичное посещение аудиторных занятий. Полное выполнение и защита заданий на практических (семинарских) занятиях. Выполнение тестовых заданий, ответы на коллоквиуме на оценки «хорошо»	Полное посещение аудиторных занятий. Полное выполнение и защита заданий на практических (семинарских) занятиях. Выполнение тестовых заданий, ответы на коллоквиуме на оценки «отлично»

– *вторая составляющая* – оценка знаний обучающегося по результатам промежуточной аттестации – зачета (до 25 баллов):

Шкала оценивания

Не зачтено (36-60 баллов)	Зачтено (61-70 баллов)
Обучающийся имеет 36-60 баллов по итогам текущего и рубежного контроля. На зачете не выполнил предложенное преподавателем задание. По итогам промежуточного контроля получил 0 баллов	Обучающийся имеет 36-50 баллов по итогам текущего и рубежного контроля, на зачете полностью выполнил одно задание и частично (полностью) второе задание. По итогам промежуточного контроля получил от 11 до 25 баллов. Обучающийся имеет 51-60 баллов по итогам текущего и рубежного контроля, на зачете выполнил одно задание полностью либо частично выполнил оба задания. По итогам промежуточного контроля получил от 1 до 10 баллов. Обучающемуся, имеющему 61-70 баллов по итогам текущего и рубежного контроля, выставляется отметка «зачтено» без сдачи зачета

5.4. Контроль курсовых работ (проектов)

Курсовая работа (проект) по дисциплине «Информационная безопасность экономической деятельности» не предусмотрена.

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

Типовые задания, обеспечивающие формирование компетенции УК-1.2 представлены в таблице 7.

Таблица 7. Результаты освоения учебной дисциплины, подлежащие проверке

Результаты обучения ***(компетенции)***	***Основные показатели оценки*** ***результатов обучения***	***Вид оценочного материала, обеспечивающие формирование компетенций***
Код и наименование компетенции выпускника УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий **Код и наименование индикатора**	***Знать:*** – основные понятия, угрозы и нормативно-правовую базу в области информационной безопасности экономической деятельности хозяйствующих субъектов, технологии обеспечения защиты корпоративной информации и управления средствами обеспечения информационной безопасности организации; – методы поиска, сбора и обработки отечественных и зарубежных источников информации и данных для решения задач обеспечения информационной безопасности	Оценочные материалы для устного опроса (раздел 5.1.1). Оценочные материалы для выполнения рефератов (раздел 5.1.2). Оценочные материалы для контрольной работы (раздел 5.1.3). Оценочные материалы для коллоквиума (раздел 5.2.1). Оценочные материалы для

достижения компетенций выпускника УК-1.2. Способен находить и критически оценивать информацию для решения проблемных ситуаций, с применением современных цифровых технологий и информационных-коммуникационных средств	организации; – процедуры анализа отечественных и зарубежных источников информации, данных и подготовки информационных обзоров и/или аналитических отчетов.	проведения тестирования (раздел 5.2.2) Оценочные материалы для промежуточной аттестации (раздел 5.3).
	Уметь: – осуществлять поиск, сбор, обработку отечественных и зарубежных источников информации и данных для целей обеспечения информационной безопасности экономической деятельности; – анализировать отечественные и зарубежные источники информации и данные, применять методы подготовки информационных обзоров и/или аналитических отчетов.	Оценочные материалы для выполнения рефератов (раздел 5.1.2). Оценочные материалы для контрольной работы (раздел 5.1.3). Оценочные материалы для промежуточной аттестации (раздел 5.3).
	Владеть: – навыками поиска, сбора, обработки отечественных и зарубежных источников информации и данных для целей обеспечения информационной безопасности экономической деятельности; – навыками анализа отечественных и зарубежных источников информации и данных, подготовки информационных обзоров и/или аналитических отчетов.	Оценочные материалы для выполнения рефератов (раздел 5.1.2). Оценочные материалы для контрольной работы (раздел 5.1.3). Оценочные материалы для промежуточной аттестации (раздел 5.3).

7. Учебно-методическое обеспечение дисциплины (модуля)

7.1. Нормативно-законодательные акты

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ. – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.

2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ. – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.

3. Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ. – [Электронный ресурс]. – Режим

доступа: Консультант Плюс: URL: www. consultant.ru.

4. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.

5. 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.

6. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.

7. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных». – [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. Внуков А.А. Защита информации [Текст] : учеб.и практ.для бакалавриата и магистратуры / А.А. Внуков. - 2-е изд., испр. и доп. - М. : Изд-во Юрайт, 2019. - 240 с. - (Бакалавр и магистр. Академический курс). - ISBN 978-5-534-01678-9. – 10 экз. (Абонемент учебной литературы – 9, Чит. зал естественных и технических наук - 1).

2. 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

3. 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

4. Морозов А.В. Информационное право и информационная безопасность. Часть 1 [Электронный ресурс] : учебник / 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

5. Морозов А.В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс] : учебник / 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

6. Организационное и правовое обеспечение информационной безопасности [Текст] : учебник и практикум

для бакалавриата и магистратуры / под ред. Т.А. Поляковой, А.А. Стрельцова. - М. : Изд-во Юрайт, 2019. - 325 с. - (Бакалавр и магистр. Академический курс). - ISBN 978-5-534-03600-8. – 10 экз. (Абонемент учебной литературы - 9, Чит. зал гуманитарных и общественных наук - 1).

7.4. Периодические издания

1.Журнал «Информационные системы и технологии». Режим доступа: http://oreluniver.ru/science/journal/isit/archive

2. Журнал «Информационная безопасность» («Information Security»). Режим доступа: http://www.itsec.ru/articles

3. Журнал «Вопросы кибербезопасности». Режим доступа: http://cyberrus.com/

2. Журнал «Компьютер пресс». – Режим доступа: https://compress.ru/technology

7.5. Интернет-ресурсы

– *профессиональные базы данных:*

1. База данных Science Index (РИНЦ). – URL: http://elibrary.ru

2. Национальная электронная библиотека РГБ (имеется режим для людей с нарушением зрения (для слепых и слабовидящих). – URL: https://нэб.рф

3. ЭБС «Лань». – URL: https://e.lanbook.com/

4. ЭБС «IPRbooks». – URL: http://iprbookshop.ru/

5. Polpred.com. Новости. Обзор СМИ. Россия и зарубежье. – URL: http://polpred.com

6. Президентская библиотека им. Б.Н. Ельцина. – URL: http://www.prlib.ru

– *информационные справочные системы:*

1. Справочная правовая система «КонсультантПлюс». – URL: www. consultant.ru

2. Портал ГАРАНТ.РУ. – URL: https://www.garant.ru

3. Портал КОНСУЛЬТАНТПЛЮС СТУДЕНТУ И ПРЕПОДАВАТЕЛЮ. – URL: www.consultant.ru/edu/

4. Портал ГАРАНТ-ОБРАЗОВАНИЕ. – URL: https://edu.garant.ru

– *иные интернет-источники:*

1. Научная электронная библиотека «Киберленинка»: https://cyberleninka.ru/

2. Сайт проекта «Security Lab», на котором помимо новостей, экспертных статей, софта, форума, есть раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению: http://www.securitylab.ru/

3. Новостной сайт об информационной безопасности «Threatpost» от Kaspersky Lab.: https://threatpos

4. Информационно-аналитический центр, посвященный информационной безопасности «Anti-Malware», проводит сравнительные тесты антивирусов, публикует аналитические статьи, эксперты принимают участие

в дискуссиях на форуме: https://www.anti-malware.ru/

5. Популярный хаб сайта Geektimes.ru про информационную безопасность, содержащий статьи, публикации о новинках индустрии: https://geektimes.ru/hub/infosecurity/

6. Раздел новостного издания о высоких технологиях CNEWS, посвященный информационной безопасности, публикуются новости и экспертные статьи: http://safe.cnews.ru/

7. «Клуб информационной безопасности» – некоммерческая организация, развивающая ИБ и решающая задачи в этой сфере. На сайте есть «База знаний», где можно найти нормативные документы, программное обеспечение, книги, ссылки на интересные ресурсы: http://wiki.informationsecurity.club/doku.php/main

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

Учебная работа по дисциплине ИБЭД состоит из контактной работы (лекции, практические занятия) и самостоятельной работы. Доля контактной учебной работы в общем объеме времени, отведенном для изучения дисциплины, составляет 38,9 % (в том числе лекционных занятий – 25,9%, практических занятий – 12,97%), доля самостоятельной работы – 52,8 %. Соотношение лекционных, семинарских и практических занятий к общему количеству часов соответствует учебному плану по специальности 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности»

Для подготовки к практическим занятиям необходимо рассмотреть контрольные вопросы, при необходимости обратиться к рекомендуемой литературе, записать непонятные моменты в вопросах для уяснения их на предстоящем занятии.

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 (семинарские) занятия способствуют углубленному изучению наиболее сложных проблем науки и служат основной формой подведения итогов самостоятельной работы обучающихся. Целью практических (семинарских) 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 (семинарскому) занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем практические задания. Следует доработать свой конспект лекции, делая в нем соответствующие записи из литературы.

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

На практических (семинарских) 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 (семинарскому) занятию зависит от формы, места его проведения, 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.

Самостоятельная работа обучающегося включает:

- изучение основной и дополнительной литературы;
- изучение материалов периодической печати и электронных ресурсов;
- подготовку к практическим (семинарским) 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.

Теоретический материал по тем темам, которые вынесены на самостоятельное изучение, обучающийся прорабатывает в соответствии с вопросами для подготовки к экзамену. Пакет заданий для самостоятельной работы выдается в начале семестра, определяются конкретные сроки их выполнения и сдачи. Результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации обучающегося. Задания для самостоятельной работы составляются, как правило, по темам и вопросам, по которым не предусмотрены аудиторные занятия, либо требуется дополнительно проработать и проанализировать рассматриваемый преподавателем материал в объеме запланированных часов.

Для закрепления теоретического материала обучающиеся выполняют различные задания (рефераты, домашние задания). Их выполнение призвано обратить внимание обучающихся на наиболее сложные, ключевые и дискуссионные аспекты изучаемой темы, помочь систематизировать и лучше усвоить пройденный материал. Такие задания могут быть использованы как для проверки знаний обучающихся преподавателем в ходе проведения занятий, а также для самопроверки знаний обучающимися.

При самостоятельном выполнении заданий обучающиеся могут выявить тот круг вопросов, который усвоили слабо, и в дальнейшем обратить на них особое внимание. Контроль самостоятельной работы обучающихся по выполнению заданий осуществляется преподавателем с помощью выборочной и фронтальной проверок на практически (семинарских) занятиях. При необходимости дополнительные консультации могут быть назначены по согласованию с преподавателем в индивидуальном порядке. Самостоятельная работа должна носить творческий и планомерный характер.

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 обучающемуся 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 студент 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.

Методические рекомендации по написанию рефератов

Реферат – доклад на определенную тему, включающий обзор соответствующих литературных и других источников; краткое изложение содержания научной работы, книги (или ее части), статьи с основными фактическими сведениями и выводами. Реферат является творческой исследовательской работой, основанной, прежде всего, на изучении значительного количества научной и иной литературы по теме исследования.

Написание реферата используется в учебном процессе в целях приобретения обучающимся 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 обучающегося 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 в отведенное для этого преподавателем время на практических занятиях. Предварительно подготовив тезисы доклада, обучающийся в течение 7 - 10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы аудитории. На основе обсуждения обучающемуся выставляется соответствующая оценка.

Методические рекомендации для подготовки к зачету

Зачет в VIII-м семестре является формой итогового контроля знаний и умений обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в процессе самостоятельной работы. Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой. К зачету допускаются студенты, набравшие 36 и более баллов по итогам текущего и промежуточного контроля. На зачете студент может набрать от 15 до 25 баллов.

В период подготовки к экзамену обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка обучающегося к зачету включает три этапа:

– самостоятельная работа в течение семестра;

– непосредственная подготовка в дни, предшествующие зачету по темам курса;

– подготовка к ответу на зачетные вопросы.

При подготовке к зачету обучающимся целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На зачет выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр, может проводится в письменной / устной форме.

При проведении зачета в письменной (устной) форме, ведущий преподаватель составляет зачетные билеты, которые могут включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня зачетных вопросов, доведенных до сведения обучающихся накануне зачетной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины. Результат устного (письменного) экзамена выражается отметкой «зачтено»

8. Материально-техническое обеспечение дисциплины

8.1. Требования к материально-техническому обеспечению

Для реализации рабочей программы дисциплины имеются учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения, а также помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КБГУ:

Перечень материально-технического обеспечения дисциплины включает в себя:

1. *Учебную аудиторию для проведения учебных занятий – 247.* Оснащена оборудованием и техническими средствами обучения (ноутбук, проектор, интерактивная доска, доска стационарная). Комплект учебной мебели – 24 посадочных места.

2. *Помещение для самостоятельной работы обучающихся – 115. Электронный читальный зал №1.* Оснащен комплектом учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде КБГУ – 28 посадочных мест. Компьютерная техника обеспечена необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Электронно-библиотечные системы и электронная информационно-образовательная среда КБГУ обеспечивают доступ (удаленный доступ) обучающимся, к современным профессиональным базам данных и информационным справочным системам.

3. *Помещение для самостоятельной работы - 311. Электронный читальный зал №3. Читальный зал естественных и технических наук.* Оснащен комплектом учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде КБГУ. 22 посадочных места. Компьютерная техника обеспечена необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Электронно-библиотечные системы и электронная информационно-образовательная среда КБГУ обеспечивают доступ (удаленный доступ) обучающимся, к современным профессиональным базам данных и информационным справочным системам.

Для проведения занятий имеется необходимый комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

- *лицензионное программное обеспечение:*
- пакет офисного программного обеспечения *Р7-Офис.Профессиональный (Десктопная версия);*
- лицензия на программное обеспечение средств антивирусной защиты *Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition;*
- право использования программного обеспечения для планирования и проведения онлайн-мероприятий (трансляций, телемостов/ аудио-видеоконференций, вебинаров) *Webinar Enterprise TOTAL 150 участников;*
- *свободно распространяемые программы:*
- программа-архиватор 7Z;
- интернет-браузеры Mozilla Firefox, Yandex;
- *информационные справочные системы:*
- «КонсультантПлюс». – URL: http://www. consultant.ru
- «Гарант» (в свободном доступе). – URL: http://www.garant.ru

8.2. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для обучающихся 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. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;

2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):

– присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ невизуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для обучающихся с нарушениями зрения;

– задания для выполнения на экзамене/зачете зачитываются ассистентом;

– письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;

3. Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):

– на экзамене/зачете присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);

– экзамен/зачет проводится в письменной форме;

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);

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

– по желанию обучающегося экзамен/зачет проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Материально-техническое обеспечение дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Аудитория для самостоятельной работы и коллективного пользования специальными техническими средствами для	Комплект учебной мебели: - столы и стулья для обучающихся (3 комплекта); - стол для инвалидов-колясочников (1 шт.);	Продукты MICROCOFT (Desktop Education ALNG LicSaPk OLVS Academic Edition Enterprise) подписка (Open Value Subscription) № V 2123829. Kaspersky Endpoint Security

обучения инвалидов и лиц с ОВЗ в КБГУ, аудитория № 145 (Главный корпус КБГУ)	- компьютер с подключением к сети и программным обеспечением (3 шт.); - специальная клавиатура (с увеличенным размером клавиш, со специальной накладкой, ограничивающей случайное нажатие соседних клавиш) (1шт.); - принтер для печати рельефно-точечным шрифтом Брайля VP Columbia (1 шт.); - портативный тактильный дисплей Брайля «Focus 14 Blue» (совместимый с планшетными устройствами, смартфонами и ПК) (1 шт.); - бумага для печати рельефно-точечным шрифтом Брайля, совместимого с принтером VP Columbia; - видеоувеличитель портативный HV-MVC, диагональ экрана – 3,5 дюйма (4 шт.); - сканирующая и читающая машина SARA-CE (1 шт.); - джойстик компьютерный адаптированный, беспроводной (3 шт.); - беспроводная Bluetooth гарнитура с костной проводимостью «AfterShokz Trekz Titanium» (1 шт.); - проводная гарнитура с костной проводимостью «AfterShokz Sportz Titanium» (2 шт.); - проводная гарнитура Defender (1 шт.); - персональный коммуникатор EN–101 (5 шт.); - специальные клавиатуры (с увеличенным размером клавиш, со специальной накладкой, ограничивающей случайное нажатие соседних клавиш); - клавиатура адаптированная с	Стандартный Russian Edition № лицензии 17E0-180427-50836-287- 197. Программы для создания и редактирования субтитров, конвертирующее речь в текстовый и жестовый форматы на экране компьютера: Майкрософт Диктейт: https://dictate.ms/, Subtitle Edit, («Сурдофон» (бесплатные). Программа невизуального доступа к информации на экране компьютера JAWS for Windows (бесплатная). Программа для чтения вслух текстовых файлов (Tiger Software Suit (TSS)) (номер лицензии 5028132082173733). Программа экранного доступа с синтезом речи для слепых и слабовидящих (NVDA) (бесплатная)

	крупными кнопками + пластиковая накладка, разделяющая клавиши, Беспроводная Clevy Keyboard + Clevy Cove (3шт.); - джойстик компьютерный Joystick SimplyWorks беспроводной (3шт.); - ноутбук + приставка для ай-трекинга к ноутбуку PCEye Mini (1 шт)	

1. Лист изменений (дополнений)

в рабочей программе дисциплины (модуля)

«Информационная безопасность экономической деятельности» по специальности 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение

экономической безопасности» на 20__- 20__ учебный год

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

Обсуждена и рекомендована на заседании кафедры экономики и учетно-аналитических информационных систем

протокол № ____ от «___» _____ 20___г.

Заведующий кафедрой _____ / А.Х. Шидов /

«__»_____20__ г.