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

УТВЕРЖДАЮ

Руководитель ОПОП
_____ Г.А. Эфендиева
«30» января 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ 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

С О Д Е Р Ж А Н И Е

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы, описание показателей, критериев оценивания компетенций на различных этапах их формирования

Карта 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 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.

Тип компетенции: общепрофессиональная компетенция выпускника образовательной программы по специальности 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности», уровень ВО – специалитет.

1.1. Этапы формирования компетенций и средства оценивания

Результаты обучения (компетенции)	Основные показатели оценки результатов обучения	Виды 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 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.	**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 организации; – процедуры анализа отечественных и зарубежных источников информации, данных и подготовки информационных обзоров и/или аналитических отчетов.	Оценочные материалы для устного опроса (раздел 3.1.1) Оценочные материалы для самостоятельной работы (раздел 3.1.2) Оценочные материалы для выполнения рефератов (раздел 3.1.3) Оценочные материалы для контрольной работы (раздел 5.1.4) Оценочные материалы для коллоквиума (раздел 5.2.1) Оценочные материалы для проведения тестирования (раздел 3.2.2) Оценочные материалы для промежуточной аттестации (раздел 3.3)
	Уметь: – осуществлять поиск, сбор, обработку отечественных и зарубежных источников информации и данных для целей обеспечения информационной безопасности экономической деятельности;	Оценочные материалы для выполнения рефератов (раздел 3.1.3) Оценочные материалы для контрольной работы (раздел 3.1.4) Оценочные материалы для промежуточной аттестации (раздел 3.3)

	– 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.	Оценочные материалы для выполнения рефератов (раздел 3.1.3) Оценочные материалы для контрольной работы (раздел 3.1.4) Оценочные материалы для промежуточной аттестации (раздел 3.3)

1.2. Критерии формирования оценок на различных этапах их формирования

Текущий и рубежный контроль

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:

Этап (уровень)	**Первый этап (уровень)**	**Второй этап (уровень)**	**Третий этап (уровень)**
Баллы	36-50 баллов	51-60 баллов	61-70 баллов
Характеристика	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»

Промежуточная аттестация (зачет)

Оценка	Не зачтено	Зачтено
Баллы	36-60 баллов	61-70 баллов
Характеристика	Обучающийся имеет 36-60 баллов по итогам текущего и рубежного контроля. На зачете не	Обучающийся имеет 36-50 баллов по итогам текущего и рубежного контроля, на зачете полностью выпол-

	выполнил предложенное преподавателем задание. По итогам промежуточного контроля получил 0 баллов	нил 1/3 и более предложенного преподавателем задания. 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 2 из трех заданий. 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

На первом (начальном) этапе формирования компетенции формируются знания, умения и навыки, составляющие базовую основу компетенции, без которой невозможно ее дальнейшее развитие. Обучающийся воспроизводит термины, факты, методы, понятия, принципы и правила; решает учебные задачи по образцу.

На втором (основном) этапе формирования компетенции приобретается опыт деятельности, когда отдельные компоненты компетенции начинают «работать» в комплексе и происходит выработка индивидуального алгоритма продуктивных действий, направленных на достижение поставленной цели. На этом этапе обучающийся осваивает аналитические действия с предметными знаниями по конкретной дисциплине, способен самостоятельно решать учебные задачи, внося коррективы в алгоритм действий, осуществляя координирование хода работы, переносит знания и умения на новые условия.

Третий (завершающий) этап – это овладение компетенцией. Обучающийся способен использовать знания, умения, навыки при решении задач повышенной сложности и в нестандартных условиях. По результатам этого этапа обучающийся демонстрирует итоговый уровень сформированности компетенции.

2. Методические материалы и типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения профессиональной образовательной программы

Примерный перечень оценочных средств

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1.	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися	Вопросы по темам/разделам дисциплины
2.	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины, представленные в привязке к компетенциям, предусмотренным РПД

3.	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося	Фонд тестовых заданий
4.	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект контрольных заданий по вариантам
5.	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее	Тема рефератов
6.	Задача (практическое задание)	Средство оценки умения применять полученные теоретические знания в практической ситуации. Задача (задание) должна быть направлена на оценивание тех компетенций, которые подлежат освоению в данной дисциплине, должна содержать четкую инструкцию по выполнению или алгоритм действий	Комплект задач и заданий

3. Перечень контрольных заданий и иных материалов, необходимых для оценки знаний, умений, навыков и опыта деятельности

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.***

3.1. 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.

3.1.1. Вопросы по темам дисциплины «Информационная безопасность экономической деятельности» (контролируемая компетенция: 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.

Тема №2. Угрозы информационной безопасности экономических субъектов

1. Раскройте понятие «угрозы нарушения целостности» информации.
2. Раскройте понятие «угрозы нарушения доступности» информации.
3. Раскройте понятие «угрозы нарушения конфиденциальности» информации.
4. Раскройте классификацию угроз информационной безопасности по природе их возникновения.

5. Раскройте классификацию угроз информационной безопасности по степени преднамеренности их возникновения.
6. Раскройте классификацию угроз информационной безопасности по источнику их возникновения.
7. Раскройте классификацию угроз информационной безопасности по положению источника их возникновения.
8. Раскройте классификацию угроз информационной безопасности по степени их зависимости от активности информационной системы.
9. Раскройте классификацию угроз информационной безопасности по степени их воздействия на информационную систему.
10. Раскройте классификацию угроз информационной безопасности по этапам доступа пользователей или программ к ресурсам информационной системы.
11. Раскройте классификацию угроз информационной безопасности по способу доступа к ресурсам информационной системы.
12. Раскройте классификацию угроз информационной безопасности по текущему месту расположения информации, хранимой и обрабатываемой в информационной системе.
13. Раскройте классификацию угроз на случайные и преднамеренные. Приведите свои примеры каждого типа угроз.
14. Раскройте понятие «гипотетическая модель потенциального нарушителя».
15. Раскройте понятие «инсайдер».
16. Раскройте понятие «несанкционированный доступ».
17. Перечислите основные каналы несанкционированного доступа.
18. Перечислите основные виды несанкционированного доступа.
19. Раскройте содержание такого вида несанкционированного доступа, как «перехват паролей».
20. Раскройте содержание такого вида несанкционированного доступа, как «маскарад».
21. Раскройте содержание такого вида несанкционированного доступа, как «незаконное использование привилегий».
22. Раскройте понятие «компьютерный вирус».
23. Перечислите виды компьютерных вирусов.
24. Раскройте понятие «сетевой червь».
25. Раскройте понятие «троянский конь».
26. Перечислите меры защиты от компьютерных вирусов.
27. Раскройте понятие «спам».
28. Раскройте понятие «сетевая атака».
29. Перечислите основные виды сетевых атак.
30. Раскройте понятие «атака доступа». Раскройте виды атак доступа.
31. Раскройте понятие «атака модификации». Раскройте виды атак модификации.
32. Раскройте понятие «атака отказа в обслуживании». Раскройте виды атак отказа в обслуживании.
33. Раскройте понятие «комбинированная атака». Раскройте виды комбинированных атак.
34. Раскройте понятие «фишинг».
35. Раскройте понятие «применение ботнетов».
36. Опишите основные угрозы безопасности в беспроводных сетях.
37. Опишите суть кибершантажа. 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.

3.1.2. Оценочные материалы для выполнения рефератов по дисциплине «Информационная безопасность экономической деятельности» (контролируемая компетенция: 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.

3.1.3. Оценочные материалы для контрольной работы по дисциплине «Информационная безопасность экономической деятельности (контролируемая компетенция: 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 курье-ром			

Контрольная работа № 2

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.

Контрольная работа № 5

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 в год, тыс. руб.	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).

3.2. 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.

3.2.1. Оценочные материалы для коллоквиума по дисциплине «Информационная безопасность экономической деятельности» (контролируемая компетенция: УК-1.2)

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 ка-

кие-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.

3.2.2. Оценочные материалы для проведения тестирования (образцы тестовых заданий) по дисциплине «Информационная безопасность экономической деятельности» (контролируемая компетенция: УК-1.2)

I: T1
S: Сфера человеческой деятельности, связанная с созданием, преобразованием и потреблением информации, называется:

-: производственная деятельность
+: информационное пространство
-: информационное общество
I: T2
S: Под проведением информационных воздействий на информационное пространство или любой его элемент в противоправных целях понимают:
+: информационная преступность
-: информационное противоборство
-: информационная война
I: T3
S: Акт применения информационного оружия – это:
-: информационное оружие
+: информационное воздействие
-: информационное противоборство
I: T4
S: Под угрозой безопасности информации понимаются:
-: информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника
-: комплекс технических и других средств, методов и технологий
+: события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы
I: T5
S: Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют:
-: компьютерный преступник
+: компьютерный пират
-: компьютерный бандит
I: T6
S: Система обеспечения безопасности информации включает подсистемы:
+: компьютерную безопасность
+: безопасное программное обеспечение
-: технику безопасности и на предприятии
I: T7
S: Под комплексом мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности понимается:
-: Политика безопасности
-: Компьютерная безопасность
+: Защита информации
I: T8
S: Документы и массивы документов в информационных системах – это …
+: информационный ресурс
-: информационный продукт
-: базы данных
I: T9
S: К числу особенностей информации как товара относят:
+: неисчерпаемость, сохраняемость, несамостоятельность
-: неисчерпаемость, сохраняемость, достоверность
-: сохраняемость, несамостоятельность, полнота
I: T10
S: Защищаемая по закону информация, доверенная или ставшая известной лицу исключительно в силу исполнения им своих профессиональных обязанностей – это …

-: служебная тайна
-: банковская тайна
+: профессиональная тайна
I: T11
S: Под сведениями о счетах клиентов и корреспондентов и действиях с ними в кредитной организации понимают:
+: тайна банковского счета
-: тайна операций по банковскому счету
-: тайна банковского вклада
I: T12
S: К профессиональной тайне относится:
+: тайна связи
-: тайца частной жизни клиента
+: тайна страхования
I: T13
S: Информация может считаться служебной тайной, если она:
+: является охраноспособной конфиденциальной информацией другого лица
-: доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей
-: информация не относится к сведениям, составляющим государственную и коммерческую тайну
I: T14
S: Сведения о принципах управления предприятием – это:
-: важные элементы системы безопасности, кодов и процедур доступа, принципы организации защиты коммерческой тайны
+: сведения о применяемых и перспективных методах управления производством
-: сведения о составе торговых клиентов, представителей и посредников; потребности в сырье, материалах, комплектующих узлах и деталях, источники удовлетворения этих потребностей; транспортные и энергетические потребности
I: T15
S: Информация может составлять коммерческую тайну, если:
-: она содержит сведения об оплачиваемой деятельности государственных служащих
-: она содержится в годовых отчетах, бухгалтерских балансах, формах 15 государственных статистических наблюдений, аудиторских заключений, а также в иных, связанных с исчислением и уплатой налогов
+: обладатель информации принимает меры к охране ее конфиденциальности.
I: T16
S: в каком году впервые стал употребляться непосредственно термин «безопасность»?
-: 1491
-: 1190
+: 1100
-: 1189
I: T17
S: Когда впервые стали употреблять термин «экономическая безопасность»?
+: во времена «великой депрессии»
-: в средние века
-: в эпоху Возрождения
-: после Второй мировой войны
I: T18
S: … — это система обеспечения устойчивости экономической системы, которая сохраняет свою целостность и способность к саморазвитию, несмотря на неблагоприятные внешние и внутренние угрозы

-: экономическая эффективность
-: социальная эффективность
+: экономическая безопасность
-: экономические интересы
I: T19
S: Основными источниками угроз информационной безопасности являются все указанное в списке:
-: хищение жестких дисков, подключение к сети, инсайдерство
+: перехват данных, хищение данных, изменение архитектуры системы
-: хищение данных, подкуп системных администраторов, нарушение регламента работы
I: T20
S: Основные объекты информационной безопасности:
+: компьютерные сети, базы данных
-: информационные системы, психологическое состояние пользователей
-: бизнес-ориентированные, коммерческие системы
I: T21
S: Угрозы экономической безопасности по характеру действия бывают:
+: нарочные
-: контролированные
-: критические
-: антропогенные
I: T22
S: К основным функциям системы безопасности можно отнести все перечисленное:
+: установление регламента, аудит системы, выявление рисков
-: установка новых офисных приложений, смена хостинг-компании
-: внедрение аутентификации, проверки контактных данных пользователей
I: T23
S: Назовите основополагающие принципы создания ЭИС:
+: системность
-: совместимость
-: развитие
-: стандартизация и унификация
I: T24
S: Информационные ресурсы являются исходной для создания:
+: информационных продуктов
-: денежных продуктов
-: материальных продуктов
I: T25
S: К числу особенностей информации как товара следует отнести:
-: самостоятельность - проявляет свою "движущую силу" только в соединении с другими ресурсами (труд, техника, сырье, энергия)
+: несамостоятельность - проявляет свою "движущую силу" только в соединении с другими ресурсами (труд, техника, сырье, энергия)
+:сохраняемость - при использовании не исчезает и даже может увеличиваться за счет трансформации полученных сообщений
I: T26
S: Информация может использоваться в организации, если удовлетворяет следующим требованиям:
+: конфиденциальность
-: не достоверность
+: оперативность использования
-: открытость

I: T27
S: Информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критерии правовой охраны):
-: к ней имеется свободный доступ на законном основании
+: обладатель информации принимает меры к охране ее конфиденциальности
I: T28
S: Какая информация подлежит защите?
-: информация, циркулирующая в системах и сетях связи
-: зафиксированная на материальном носителе информация с реквизитами,
-: позволяющими ее идентифицировать
-: только информация, составляющая государственные информационные ресурсы
+: любая документированная информация, неправомерное обращение с которой
+: может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу
I: T29
S: Формы защиты интеллектуальной собственности
+: авторское, патентное право и коммерческая тайна
-: интеллектуальное право и смежные права
-: гражданское и административное право
I: T30
S: Виды информационной безопасности:
+: Персональная, корпоративная, государственная
-: Клиентская, серверная, сетевая
-: Локальная, глобальная, смешанная
I: T31
S: Цели информационной безопасности – своевременное обнаружение, предупреждение:
+: несанкционированного доступа, воздействия в сети
-: инсайдерства в организации
-: чрезвычайных ситуаций
I: T32
S: К правовым методам, обеспечивающим информационную безопасность, относятся:
-: разработка аппаратных средств обеспечения правовых данных
-: разработка и установка во всех компьютерных правовых сетях журналов учета действий
+: разработка и конкретизация правовых нормативных актов обеспечения безопасности
I: T33
S: Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
-: регламентированной
-: правовой
+: защищаемой
I: T34
S: Наиболее важным при реализации защитных мер политики безопасности является:
-: аудит, анализ затрат на проведение защитных мер
-: аудит, анализ безопасности
+: аудит, анализ уязвимостей, риск-ситуаций
I: T35
S: Информация это -
-: сведения, поступающие от СМИ
-: только документированные сведения о лицах, предметах, фактах, событиях
+: сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
-: только сведения, содержащиеся в электронных базах данных
I: T36

S: Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется:
-: достоверной
-: конфиденциальной
+: документированной
-: коммерческой тайной
I: T37
S: По принадлежности информационные ресурсы подразделяются на
+: государственные, коммерческие и личные
-: государственные, не государственные и информацию о гражданах
-: информацию юридических и физических лиц
-: официальные, гражданские и коммерческие
I: T38
S: По доступности информация классифицируется на
-: открытую информацию и государственную тайну
-: конфиденциальную информацию и информацию свободного доступа
+: информацию с ограниченным доступом и общедоступную информацию
-: виды информации, указанные в остальных пунктах
I: T39
S: К конфиденциальной информации относятся документы, содержащие
+: государственную тайну
-: законодательные акты
-: "ноу-хау"
-: сведения о золотом запасе страны
I: T40
S: Запрещено относить к информации ограниченного доступа
-: информацию о чрезвычайных ситуациях
-: информацию о деятельности органов государственной власти
-: документы открытых архивов и библиотек
+: все, перечисленное в остальных пунктах
I: T41
S: К конфиденциальной информации не относится
-: коммерческая тайна
-: персональные данные о гражданах
-: государственная тайна
+: "ноу-хау"
I: T42
S: Вопросы информационного обмена регулируются (...) правом
+: гражданским
-: информационным
-: конституционным
-: уголовным
I: T43
S: Согласно ст.132 ГК РФ интеллектуальная собственность это
-: информация, полученная в результате интеллектуальной деятельности индивида
-: литературные, художественные и научные произведения
-: изобретения, открытия, промышленные образцы и товарные знаки
+: исключительное право гражданина или юридического лица на результаты
+: интеллектуальной деятельности
I: T44
S: Интеллектуальная собственность включает права, относящиеся к
-: литературным, художественным и научным произведениям, изобретениям и

открытиям
-: исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
-: промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям
+: всему, указанному в остальных пунктах
I: Т45
S: Какая информация подлежит защите?
-: информация, циркулирующая в системах и сетях связи
-: зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
-: только информация, составляющая государственные информационные ресурсы
+: любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу
I: Т46
S: Классификация и виды информационных ресурсов определены
+: Законом "Об информации, информатизации и защите информации"
-: Гражданским кодексом
-: Конституцией
-: всеми документами, перечисленными в остальных пунктах
I: Т47
S: Запрещено относить к информации с ограниченным доступом
+: законодательные акты, информацию о чрезвычайных ситуациях и информацию о деятельности органов государственной власти (кроме государственной тайны)
-: только информацию о чрезвычайных ситуациях
-: только информацию о деятельности органов государственной власти, (кроме государственной тайны)
-: документы всех библиотек и архивов
I: Т48
S: Формой правовой защиты изобретений является
-: институт коммерческой тайны
+: патентное право
-: авторское право
-: все, перечисленное в остальных пунктах
I: Т49
S: Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности?
+: да
-: нет
-: только авторское и патентное
-: только КТ
I: Т50
S: К государственной тайне относится...
-: информация в военной области
-: информация о внешнеполитической и внешнеэкономической деятельности государства
-: информация в области экономики, науки и техники и сведения в области разведывательной и оперативно-розыскной деятельности
+: все выше перечисленное
I: Т 51
S: Гриф "ДСП" используется
-: для секретных документов
-: для документов, содержащих коммерческую тайну
+: как промежуточный для несекретных документов

-: в учебных целях
I: T52
S: Основная масса угроз информационной безопасности приходится на:
+: Троянские программы
-: Шпионские программы
-: Черви
I: T53
S: Информационная безопасность зависит от:
+: компьютеров, поддерживающей инфраструктуры
-: пользователей
-: информации
I: T54
S: Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+: владелец сети
-: администратор сети
-: пользователь сети
I: T55
S: Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
-: регламентированной
-: правовой
+: защищаемой
I: T56
S: Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+: целостность
-: доступность
-: актуальность
I: T57
S: Утечкой информации в системе называется ситуация, характеризуемая:
+: потерей данных в системе
-: изменением формы информации
-: изменением содержания информации
I: T58
S: Наиболее распространены средства воздействия на сеть офиса:
-: слабый трафик, информационный обман, вирусы в интернет
+: вирусы в сети, логические мины (закладки), информационный перехват
-: компьютерные сбои, изменение администрирования, топологии
I: T59
S: Наиболее распространены угрозы информационной безопасности корпоративной системы:
-: покупка нелицензионного ПО
+: ошибки эксплуатации и неумышленного изменения режима работы системы
-: сознательного внедрения сетевых вирусов
I: T60
S: Наиболее распространены угрозы информационной безопасности сети:
-: распределенный доступ клиент, отказ оборудования
-: моральный износ сети, инсайдерство
+: сбой (отказ) оборудования, нелегальное копирование данных
I: T61
S: Принципом политики информационной безопасности является принцип:
+: разделения доступа (обязанностей, привилегий) клиентам сети (системы)

-: одноуровневой защиты сети, системы
-: совместимых, однотипных программно-технических средств сети, системы
I: T62
S: Принципом информационной безопасности является принцип недопущения:
+: неоправданных ограничений при работе в сети (системе)
-: рисков безопасности сети, системы
-: презумпции секретности
I: T63
S: К основным функциям системы безопасности можно отнести все перечисленное:
+: установление регламента, аудит системы, выявление рисков
-: установка новых офисных приложений, смена хостинг-компании
-: внедрение аутентификации, проверки контактных данных пользователей
I: T64
S: К основным принципам обеспечения информационной безопасности относится:
+: экономической эффективности системы безопасности
-: много платформенной реализации системы
-: усиления защищенности всех звеньев системы
I: T65
S: Основными рисками информационной безопасности являются:
-: искажение, уменьшение объема, перекодировка информации
-: техническое вмешательство, выведение из строя оборудования сети
+: потеря, искажение, утечка информации
I: T66
S: Под информационной безопасностью понимается…
+: защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре.
-: программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
-: нет правильного ответа
I: T67
S: Для чего создаются информационные системы?
+: получения определенных информационных услуг
-: обработки информации
-: все ответы правильные
I: T68
S: Что является определением воздействия (exposure) на безопасность?
+: нечто, приводящее к ущербу от угрозы
-: любая потенциальная опасность для информации или систем
-: любой недостаток или отсутствие информационной безопасности
-: потенциальные потери от угрозы
I: T69
S: Угроза – это…
+: потенциальная возможность определенным образом нарушить информационную безопасность
-: система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
-: процесс определения отвечает на текущее состояние разработки требованиям данного этапа
I: T70
S: Вирус – это…

+: код обладающий способностью к распространению путем внедрения в другие программы
-: способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
-: небольшая программа для выполнения определенной задачи
I: T71
S: Предпосылки появления угроз:
+: объективные
+: субъективные
-: преднамеренные
I: T72
S: СЗИ (система защиты информации) делится:
+: ресурсы автоматизированных систем
+: организационно-правовое обеспечение
-: человеческий компонент
I: T73
S: Основополагающие документы для обеспечения безопасности внутри организации:
+: трудовой договор сотрудников
+: должностные обязанности руководителей
-: коллективный договор
I: T74
S: Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
+: поддержка высшего руководства
-: эффективные защитные меры и методы их внедрения
-: актуальные и адекватные политики и процедуры безопасности
-: проведение тренингов по безопасности для всех сотрудников
I: T75
S: Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
-: Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
-: когда риски не могут быть приняты во внимание по политическим соображениям
-: когда необходимые защитные меры слишком сложны
+: когда стоимость контрмер превышает ценность актива и потенциальные потери
I: T76
S: Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
-: внедрение управления механизмами безопасности
-: классификацию данных после внедрения механизмов безопасности
+: уровень доверия, обеспечиваемый механизмом безопасности
-: соотношение затрат / выгод
I: T77
S: Защита информации от утечки — это деятельность по предотвращению:
-: воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
+: неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа
I: T78
S: Естественные угрозы безопасности информации вызваны:
+: воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
-: корыстными устремлениями злоумышленников;

-: ошибками при действиях персонала.
I: T79
S: с каким понятием связан термин «угроза» с правовой точки зрения?
-: квалификация
+: ущерб
-: утрата
-: доступность
I: T80
S: Какие составляющие относятся к информационно-технологическому ресурсу современного предприятия?
+: внешняя и внутренняя информация
+: обслуживающие системы и технологии
-: весь персонал
+: ИТ-специалисты и персонал ИТ-подразделений
-: финансовый капитал
I: T81
S: К какой категории охраняемой информации относится государственная тайна?
-: государственная тайна
-: служебная тайна
+: профессиональная тайна
-: объекты авторского права
I: T82
S: К внутренним нарушителям информационной безопасности относится:
-: любые лица, находящиеся внутри контролируемой территории;
-: представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
-: персонал, обслуживающий технические средства.
-: сотрудники отделов разработки и сопровождения ПО;
+: технический персонал, обслуживающий здание
I: T83
S: Перехват, который осуществляется путем использования оптической техники называется:
-: активный перехват;
-: пассивный перехват;
-: аудиоперехват;
+: видеоперехват;
-: просмотр мусора
I: T84
S: Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
-: пассивный перехват;
+: аудиоперехват;
-: видеоперехват;
-: просмотр мусора
I: T85
S: Активный перехват информации — это перехват, который:
-: неправомерно использует технологические отходы информационного процесса;
-: осуществляется путем использования оптической техники;
+: осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера
I: T86

S: Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….
+: информационная война
-: информационное оружие
-: информационное превосходство
I: T87
S: Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.
-: служебная информация
-: коммерческая тайна
-: банковская тайна
+: конфиденциальная информация
I: T88
S: Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
+: конфиденциальность
-: целостность
-: доступность
-: аутентичность
-: аппелеруемость
I: T89
S: Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано
+: надежность
-: точность
-: контролируемость
-: устойчивость
-: доступность
I: T90
S: Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
-: принцип системности
-: принцип комплексности
-: принцип непрерывной защиты
-: принцип разумной достаточности
+: принцип гибкости системы
I: T91
S: В классификацию вирусов по способу заражения входят
-: опасные
-: файловые
+: резидентные
-: загрузочные
-: файлово -загрузочные
+: нерезидентные
I: T92
S: К принципам информационной безопасности относятся
-: скрытость
-: масштабность
+: системность

+: законность
+: открытости алгоритмов
I: T93
S: Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…
+: защита информации
-: компьютерная безопасность
-: защищенность информации
-: безопасность данных
I:T94
S: Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
информационная война
+: информационное оружие
-: информационное превосходство
I: T95
S: К функциям информационной безопасности относятся:
+: совершенствование законодательства РФ в сфере обеспечения информационной безопасности
+: выявление источников внутренних и внешних угроз
+: страхование информационных ресурсов
+: защита государственных информационных ресурсов
+: подготовка специалистов по обеспечению информационной безопасности
I: T96
S: Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:
-: информационные ресурсы
-: информационная система
-: информационная сфера
-: информационные услуги
+: информационные продукты
I: T97
S: Действие субъектов по обеспечению пользователей информационными продуктами:
-: информационные ресурсы
-: информационная система
-: информационная сфера
+: информационные услуги
-: информационные продукты
I: T98
S: Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:
-: защита информации от непреднамеренного воздействия
-: защита информации от несанкционированного воздействия
-: защита информации от несанкционированного доступа
+: защита от утечки информации
I: T99
S: Состояние защищенности, при котором не угрожает опасность это:
-: Информационная безопасность
+: Безопасность

-: Защита информации
-: Национальная безопасность
I: T100
S: Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.
+: государственная тайна
-: коммерческая тайна
-: банковская тайна
-: конфиденциальная информация

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

3.3. 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.

3.3.1. Вопросы к зачету (контролируемая компетенция: 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.

3.3.2. Примеры типовых контрольных заданий на зачете (контролируемая компетенция: 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.

Вы – сотрудник фармацевтического учреждения. Ежедневно в базе данных происходит накопление большого количества информации.

1. Перечислите возможные способы способом обеспечения целостности и предотвращения уничтожения данных.
2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему.

Ответ к задаче №1:

1. Резервное копирование, архивирование.

2. В случае резервного копирования речь идет о кратко- или среднесрочном дополнительном хранении данных, которые еще могут понадобиться пользователям в их работе. Если, например, в результате повреждения жесткого диска или по иным причинам текущие данные теряются, их удастся быстро восстановить. Так можно эффективно защитить данные от разного рода случайностей. Время хранения резервных копий массива данных устанавливается не слишком продолжительное – несколько недель или месяцев.

Архивированию, напротив, подвергаются данные, которые из категории активно используемых перешли в «статичное» состояние, поэтому к ним обращаются сравнительно редко. Их можно уже извлечь из резервной копии и сохранить в архиве. Оба подхода различаются и уровнем затрат на приобретение необходимых технических средств: для архивирования большого объема данных применяются, как правило, недорогие носители с высокой емкостью хранения, например, оптические носители.

В описанной выше ситуации необходимо осуществлять резервное копирование данных.

КОНТРОЛЬНОЕ ЗАДАНИЕ 2.

На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника.

1. Какие правила обеспечения информационной безопасности нарушены?
2. Какие символы должны быть использованы при записи пароля?

Ответ к задаче №2:

1. Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рожде-

ния своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

2. В качестве пароля должна выбираться последовательность символов, обеспечивающая малую вероятность её угадывания. Пароль должен легко запоминаться.

КОНТРОЛЬНОЕ ЗАДАНИЕ 3.

Вы – начальник информационной службы в ООО «Прогресс». У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?
2. Какое наказание должен понести нарушитель?

Ответ к задаче №3:

1. Статья 272. Неправомерный доступ к компьютерной информации.
2. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

КОНТРОЛЬНОЕ ЗАДАНИЕ 4.

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 5.

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 6.

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 ЗАДАНИЕ74.

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 8.

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 9.

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

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

Форма билета для зачета
по учебной дисциплине

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

Дисциплина Коммерческая тайна и методы защиты конфиденциальной информации

БИЛЕТ № 1

Вопрос 1. Основные понятия информационной безопасности.
Вопрос 2. Анализ корпоративной системы с традиционной структурой**.**
3. Задача: Вы – сотрудник фармацевтического учреждения. Ежедневно в базе данных происходит накопление большого количества информации.
1. Перечислите возможные способы способом обеспечения целостности и предотвращения уничтожения данных.
2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему**?**

Руководитель ОПОП_____Г.А. Эфендиева

Заведующий кафедрой_____А.Х. Шидов