Приложение 6
к основной профессиональной образовательной программе
по направлению подготовки 38.03.06 Торговое дело
направленность (профиль) программы Торговый менеджмент
и маркетинг (во внутренней и внешней торговле)

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»

Факультет экономики, менеджмента и торговли

Кафедра экономики и цифровых технологий

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине «Основы информационной безопасности»

Направление подготовки 38.03.06 Торговое дело

направление (профиль) программы
Торговый менеджмент и маркетинг (во внутренней и внешней торговле)

Уровень высшего образования Бакалавриат

Год начала подготовки 2025

Краснодар – 2024 г.

Составитель:

к.п.н, доцент В.В. Салий

Оценочные материалы одобрены на заседании кафедры экономики и цифровых технологий
Протокол № 9 от «14» марта 2024 г.

ОЦЕНОЧНЫЕ СРЕДСТВА

По дисциплине «Основы информационной безопасности»

ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ И ЭТАПОВ ИХ ФОРМИРОВАНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции (*код и наименование компетенции*)	**Индикаторы достижения компетенций (*код и наименование индикатора*)**	**Результаты обучения *(знания, умения)***
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	**УК-1.1**. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	**УК-1.1. З-1. Знает** основные методы критического анализа и основы системного подхода как общенаучного метода.
		УК-1.1. У-1. Умеет анализировать задачу, используя основы критического анализа и системного подхода.
		УК-1.1. У-2. Умеет осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Перечень учебных заданий на аудиторных занятиях

Темы групповых дискуссий

Тема 1. Информация как объект защиты. Правовое обеспечение информационной безопасности
Индикаторы достижения: УК-1.1.

1. Информационная безопасность. Основные понятия.
2. Модели информационной безопасности.
3. Виды защищаемой информации.
4. Основные нормативно-правовые акты в области информационной безопасности.

5. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.
6. Ресурсы предприятия, подлежащие защите с точки зрения ИБ.
7. Аспекты ИБ в рамках менеджмента непрерывности бизнеса
8. Кибербезопасность и киберпространство..
9. Задачи кибербезопасности в автоматизированных системах.
10. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз.

Тема 2. Организационное обеспечение информационной безопасности

Индикаторы достижения: УК-1.1.

1. Основные стандарты в области обеспечения информационной безопасности.
2. Политика безопасности.
3. Экономическая безопасность предприятия.
4. Инженерная защита объектов.
5. Защита информации от утечки по техническим каналам.
6. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
7. Идентификация и оценка активов.
8. Модели угроз.
9. Идентификация уязвимостей.
10. Оценка рисков.
11. Обработка рисков.
12. Модель нарушителя политики безопасности.
13. Типичные угрозы информации и уязвимости корпоративных информационных систем.

Тема 3. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях
Индикаторы достижения: УК-1.1.

1. Основные виды сетевых и компьютерных угроз.
2. Средства и методы защиты от сетевых компьютерных угроз.
3. Симметричные и ассиметричные системы шифрования.
4. Цифровые подписи (Электронные подписи).
5. Инфраструктура открытых ключей.
6. Криптографические протоколы.
7. Хэш-функция и электронная подпись и протоколы электронных данных.
8. Методы работы с программными средствами.

9. Финансовые автоматизированные информационные системы управления процессами.
10. Сбор экономической разведывательной информации.
11. Топология киберпространства
12. Принципы построения архитектуры финансовой кибербезопасности.
13. Аппаратное обеспечение и хранение передаваемых и получаемых данных.
14. Протоколы и платформы.
15. Архитектура сетевой безопасности и управление процессом обеспечения безопасности.
16. Требования к системам защиты информации.

Тема 4. Стандарты и спецификации в области информационной безопасности

Индикаторы достижения: УК-1.1.

1. Стандартизация в сфере управления информационной безопасностью (на основе международных стандартов ISO/IEC 17799, ISO/IEC27002, ISO/IEC27001,ISO/IEC 15408).
2. Создание зашифрованных файлов и криптоконтейнеров и их расшифровывание.
3. Соответствие требованиям законодательства по информационной безопасности организации.
4. Соответствие политикам безопасности и стандартам, техническое соответствие.
5. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.
6. Протоколы сетевой безопасности.
7. Виртуализация сетевых устройств.
8. Управление экономическими объектами на основе стандартов информационной безопасности.

Критерии оценки (в баллах):

20 баллов выставляется обучающемуся, если он демонстрирует высокий уровень владения материалом по всем темам дискуссий,превосходное умение формулировать свою позицию, отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения, высокий уровень этики ведения дискуссии. Уровень сформированности компетенций соответствует продвинутому уровню;

15- баллов выставляется обучающемуся, если он демонстрирует владение материалом по всем темам дискуссий на уровне выше среднего, умение отстаивать её в споре, задавать вопросы, обсуждать дискуссионные положения,

знание этики ведения дискуссии. Уровень сформированности компетенций соответствует повышенному уровню;

10 баллов выставляется обучающемуся, если он демонстрирует владение материалом по всем темам дискуссий не в полном объеме, умение задавать вопросы, обсуждать дискуссионные положения, знание этики ведения дискуссии. Уровень сформированности компетенций соответствует базовому уровню.

Контрольная работа

По теме 4. Стандарты и спецификации в области информационной безопасности

Индикаторы достижения: УК-1.1.

1. Классификация мер обеспечения безопасности компьютерных систем?
2. Задачи, которые должны решаться системой защиты информации?
3. Основные принципы построения систем защиты АСОИ?
4. Основные механизмы защиты компьютерных систем от проникновения с цельюдезорганизации их работы и НСД к информации?
5. Методы обеспечения информационной безопасности РФ?
6. Организационные методы информационной безопасности?
7. Направления защиты информационной системы?
8. Этапы создания системы защиты информации?
9. Основные организационные мероприятия?
10. Средства защиты от несанкционированного доступа?
11. Мандатное управление доступом?
12. Избирательное управление доступом?
13. Управление доступом на основе ролей?
14. Системы анализа и моделирования информационных потоков?
15. Защита информации от побочного электромагнитного излучения и наводок?
16. Анализаторы протоколов?
17. Межсетевые экраны?
18. Системы резервного копирования?
19. Системы бесперебойного питания?
20. Системы аутентификации?
21. Биометрические технологии?
22. Технология единого входа?
23. Средства контроля доступа?
24. Организация информационной безопасности компании?
25. Выбор средств информационной безопасности?
26. Информационное страхование?
27. Стандартизация в сфере управления информационной

безопасностью (на основе международных стандартов ISO/IEC 17799, ISO/IEC27002, ISO/IEC27001,ISO/IEC 15408).

28. Создание зашифрованных файлов и криптоконтейнеров и их расшифровывание.
29. Соответствие требованиям законодательства по информационной безопасности организации.
30. Соответствие политикам безопасности и стандартам, техническое соответствие.
31. Перечислите критерии классификации уязвимостей.
32. Дайте определение политики безопасности.
33. Как выглядит цепочка реакций для построения системы защиты от атак?
34. Дайте определение компьютерного вируса.
35. Сформулируйте основные угрозы для персонального компьютера.
36. Дайте определение идентификации и аутентификации.
37. В чем суть утечки по каналу ПЭМИН?
38. В чем суть утечки по цепям питания и заземления?

Критерии оценки (в баллах):

10 баллов выставляется обучающемуся, если он правильно ответил на 80% вопросов (компетенция сформирована на продвинутом уровне);

9 баллов выставляется обучающемуся, если он правильно ответил на 70% вопросов (компетенция сформирована на продвинутом уровне);

8 баллов выставляется обучающемуся, если он правильно ответил на 60% вопросов теста (компетенция сформирована на повышенном уровне);

7 баллов выставляется обучающемуся, если он правильно ответил на 55% вопросов теста (компетенция сформирована на повышенном уровне);

6 баллов выставляется обучающемуся, если он правильно ответил на 50% вопросов теста (компетенция сформирована на базовом уровне)

Задания для текущего контроля

Комплект тестовых заданий по дисциплине

Индикаторы достижения: УК-1.1.

1. Контрольные функции в области государственной безопасности по вопросам предотвращения несанкциониров анного доступа к информации реализуются:

а. ФСТЭК РФ

б. ФСБ РФ

в. Управлением «К» МВД РФ

г. Федеральной службой по надзору в сфере связи, информационны х

технологий и массовых коммуникаций

2. Защита информации от несанкционированного доступа -это:

а. защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленными нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемойинформации

б. деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

в. защита информации, заключающаяся в обеспечении некриптографическими методами

безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательств ом, с применением технических, программных и программно- технических средств

г. защита информации с помощью ее криптографическ ого преобразования

3. Несанкционированный доступ кинформации – это…

а. доступ к информации ресурсам информационной системы, осуществляем ый с нарушением установленных прав и/или правил доступа к информации ресурсам информационной системы с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам

б. неконтролируемое распространение е информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

в. неправомерное получение информации с использованием технического средства, осуществляющего обнаружение,прием и обработку информативных

г. изменение, уничтожение или копирование информации (ресурсов информационной системы), осуществляемое с нарушением установленных прав и (или) правил

4. Информационное право составляет:
- нормативную базу информационного общества
- государственную политику
- нормативную базу аграрного общества
- нормативную базу до индустриального общества

5. Кто такие "кибersквоттеры"?
- сетевые деятели, пытающиеся вести паразитическое существование
- вирусы
- роботы в сети
- сетевые группы по интересам

6. На чем основан принцип работы антивирусных иммунизаторов?

- На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные

- На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски

- На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.

- На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю

7. Что необходимо сделать при обнаружении файлового вируса?

- Компьютер необходимо отключить от сети и проинформировать системного администратора

- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

29. Что необходимо сделать при обнаружении загрузочного вируса?

- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

- Компьютер необходимо отключить от сети и проинформировать системного администратора

- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

8. Что необходимо сделать при обнаружении макровируса?

- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

- Компьютер необходимо отключить от сети и проинформиравать системного администратора

- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются

9. В чем заключается метод защиты - ограничение доступа?

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. приведении её к неявному виду

10. В чем заключается метод защиты информации - разграничение доступа?

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

11.В чем заключается метод защиты информации - разделение доступа (привилегий)

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

12. В чем заключается криптографическое преобразование информации?

- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями

- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы

13. Что означает термин БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

- Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию.

- Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

- Защищенность информации от нежелательного её разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного её тиражирования

14. Кто является хакером?

- Это лица, проявляющие чрезмерный интерес к устройству сложных систем и обладающие большими познаниями по части архитектуры и принципов устройства вычислительной среды или технологии телекоммуникаций, что используется для похищения информации.

- Это лица, изучающие систему с целью её взлома. Они реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения и вирусов, используют принципы построения протоколов сетевого обмена.

- Это лица, которые "взламывая" интрасети, получают информацию о топологии этих сетей, используемых в них программно-аппаратных средствах и информационных ресурсах. Эти сведения они продают заинтересованным лицам

15. Что означает термин УЯЗВИМОСТЬ ИНФОРМАЦИИ?

- Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности, или неправомерному её тиражированию.

- Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

- Это свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию)

16. чем заключается конфиденциальность компонента системы?

- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.
- В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.
- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

17. В чем заключается целостность компонента системы?

- В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.
- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.
- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

40. В чем заключается доступность компонента системы?

- В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.
- В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.
- В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

18. Что означает термин ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.
- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.
- Это меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов.

19. Что означает термин МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

20. Что означает термин ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а так же порядок взаимодействия пользователей с системой.

- Это действующие в стране законы, указы и другие нормативные акты.

- Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

21. Что означает термин ФИЗИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

- Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.

- Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

- Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

22. Что означает термин АУТЕНТИФИКАЦИЯ?

- Это проверка подлинности объекта или субъекта
- Это проверка целостности информации, программы, документа
- Это присвоение имени субъекту или объекту

23. Что означает термин ВЕРИФИКАЦИЯ?

- Это проверка целостности информации, программы, документа.
- Это проверка подлинности субъекта или объекта.
- Это присвоение имени субъекту или объекту.

24. Что означает термин ИДЕНТИФИКАЦИЯ?

- Это присвоение имени субъекту или объекту.
- Это проверка подлинности субъекта или объекта.
- Это проверка целостности информации, программы, документа.

25. Что означает термин КРИПТОГРАФИЯ?

- Это метод специального преобразования информации с целью сокрытия от посторонних лиц

- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода

- Это преобразование информации при её передаче по каналам связи от одного элемента вычислительной сети к другому

26. Что означает термин КОДИРОВАНИЕ ИНФОРМАЦИИ?

- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода.

- Это метод специального преобразования информации с целью сокрытия от посторонних лиц.

- Это криптографическое преобразование информации при её передаче по каналам связи от одного элемента в вычислительной сети к другому.

27. Что означает термин ЛИНЕЙНОЕ ШИФРОВАНИЕ?

- Это криптографическое преобразование информации при её передаче по каналам связи от одного элемента вычислительной сети к другому.

- Это метод специального преобразования информации с целью сокрытия от посторонних лиц.

- Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода.

28. Как классифицируются виды угроз информации по природе возникновения?

- Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования.

- Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным.

- Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования.

29. Как классифицируются виды угроз информации по ориентации на ресурсы?

- Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным.

- Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования.

- Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования.

30. Какие угрозы относятся к естественным?

- Отказы и сбои аппаратуры; Помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия.
- Ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков структурные, алгоритмические и программные ошибки; действия

человека, направленные на несанкционированные воздействия на информацию.

- Аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков

31. Какие угрозы информации относятся к искусственным?

- Ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков; структурные, алгоритмические и программные ошибки; действия человека, направленные на несанкционированные воздействия на информацию
- Отказы и сбои аппаратуры; помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия
- Аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков

32. Какие угрозы информации относятся к случайным?

- Проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неумышленная порча носителей информации.
- Несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.
- Пересылка данных по ошибочному адресу абонента; ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.

33. Какие угрозы информации относятся к преднамеренным?

- Несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.
- Проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение

средств защиты персоналом службы безопасности; неправомерное включение оборудования или изменение режимов работы устройств и программ.

- Пересылка данных по ошибочному адресу абонента; ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы

34. Какими основными свойствами обладает компьютерный вирус?

- Способностью к созданию собственных копий; наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.
- Способностью к созданию собственных копий; способностью уничтожать информацию на дисках; способностью создавать всевозможные видео и звуковые эффекты.
- Наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы; способностью оставлять в оперативной памяти свою резидентную часть; способностью вируса полностью или частично скрыть себя в системе.

35. Как классифицируются вирусы в зависимости от среды обитания?

- Файловые; загрузочные; макровирусы; сетевые.
- ЗаражающиеDOS, Windows, Word, Excel,Office.
- Безвредные; неопасные; опасные.
- тОчень опасные.

36. Как классифицируются вирусы в зависимости от заражаемой ОС?

- Заражающие DOS, Windows, Word, Excel, Office
- Файловые; загрузочные; макровирусы; сетевые.
- Безвредные; неопасные; опасные; очень опасные.
- Использование резидентности, использование "стелс"-алгоритмов;
- Использование самошифрование и полиморфичность; использование нестандартных приемов

37. Как классифицируются вирусы в зависимости от особенностей алгоритма работы?

- Использование резидентность; использование "стелс"-алгоритмов; использование самошифрование и полиморфичность; использование нестандартных приемов.
- Файловые; загрузочные; макровирусы; сетевые
- Заражающие DOS, Windows, ,Word, Excel, Office
- Безвредные; неопасные; опасные; очень опасные

38. Какие программы относятся к программам Конструкторы вирусов?

- Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.

- Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п.

- Это программы, которые на первый взгляд являются стопроценными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса.

- Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика

Критерии оценки (в баллах):

10 баллов выставляется обучающемуся, если он правильно ответил на 30 вопросов теста (компетенция сформирована на продвинутом уровне);

9 баллов выставляется обучающемуся, если он правильно ответил на 27 вопросов теста (компетенция сформирована на продвинутом уровне);

8 баллов выставляется обучающемуся, если он правильно ответил на 23 вопросов теста (компетенция сформирована на повышенном уровне);

7 баллов выставляется обучающемуся, если он правильно ответил на 20 вопросов теста (компетенция сформирована на повышенном уровне);

6 баллов выставляется обучающемуся, если он правильно ответил на 18 вопросов теста (компетенция сформирована на базовом уровне)

5 баллов выставляется обучающемуся, если он правильно ответил на 15 вопросов теста (компетенция сформирована на базовом уровне).

Типовые практические задания

Индикаторы достижения: УК-1.1.

Задание 1.

Поиск источников информации в сети Интернет: открытые и закрытые источники данных. Портал открытых данных РФ. Сохранение данных в программе Excel. Преобразование и первичная обработка данных.

Задание 2.

Безопасность информационных систем

Вопросы:

1. Что вы представляете под безопасностью информационный системы.
2. Что относиться к основным характеристикам защищаемой

информации?

3. Что вы отнесете к информации ограниченного доступа?

4. По каким направлениям будет осуществляться дальнейшее развитие системыинформационной безопасности в РФ?

Задание:

Определите в каких формах представлена информация на вашем домашнем компьютере.

Опишите как обеспечивается информационная безопасность на вашем домашнем компьютере и отвечает ли современным требованиям развития систем безопасности.

Задание № 3

Анализ рисков информационной безопасности

1. Загрузите ГОСТ Р ИСО/МЭК ТО 27005
2. Ознакомьтесь с Приложениями C, D и E ГОСТ.
3. Выберите три различных информационных актива организации (см. вариант).
4. Из Приложения D ГОСТ подберите три конкретных уязвимости системы защитыуказанных информационных активов.
5. Пользуясь Приложением C ГОСТ напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь одним из методов (см. вариант) предложенных в Приложении E ГОСТпроизведите оценку рисков информационной безопасности.
7. Оценку ценности информационного актива производить на основании возможныхпотерь для организации в случае реализации угрозы.

Номер варианта	Организация	Метод оценки риска (см. Приложение EГОСТ)
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4
9	Аудиторская компания	1
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
12	Офис адвоката	4
13	Компания по разработке ПО для сторонних организаций	1

14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
17	Издательство	1
18	Консалтинговая фирма	2
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
22	Бюро перевода (документов)	2
23	Научно проектное предприятие	3
24	Брачное агентство	4
25	Редакция газеты	1
26	Гостиница	2
27	Праздничное агентство	3
28	Городской архив	4
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

Задание № 4.

Разработка частной детализированной политики ОИБ

Цель работы: ознакомление с основными частными политиками ОИБ.

Порядок выполнения работы: Определить требования обеспечивающие эффективное ОИБ, которые должны выполняться сотрудниками организации в рамках выполнения своих служебных обязанностей

Номер варианта	Организация	Детализированная политика ИБ
1	Отделение коммерческого банка	Организация режима секретности
2	Поликлиника	Физическая защита
3	Колледж	Транспортировка носителей информации
4	Офис страховой компании	Опубликование материалов в открытых источниках
5	Рекрутинговое агентство	Доступ сторонних пользователей в информационные системы организации
6	Интернет-магазин	Оценки рисков
7	ентр оказания государственных услуг	Управления паролями
8	Отделение полиции	Доступ к конфиденциальной информации
9	Аудиторская компания	Использования Интернет
10	Дизайнерская фирма	Установка и обновление ПО
11	Офис интернет-провайдера	Политика использования электронной почты

12	Офис адвоката	Использование мобильных аппаратных средств обработки информации
13	Компания по разработке ПО для сторонних организаций	Разработка и лицензирование ПО
14	Агентство недвижимости	Удалённый доступ к информационной системе.
15	Туристическое агентство	Использование отдельных универсальных информационных технологий в масштабе организации
16	Офис благотворительного фонда	Проведение аудита ИБ
17	Издательство	Антивирусная защита
18	Консалтинговая фирма	Резервное копирование
19	Рекламное агентство	ИБ при электронном документообороте
20	Отделение налоговой службы	Техническая защита информации
21	Офис нотариуса	Реагирование на инциденты ИБ
22	Бюро перевода (документов)	Проведение служебных расследований
23	Строительное предприятие	Защита научно-технической информации
24	Брачное агентство	Контроль пользователей при работе с внешними источниками информации
25	Редакция газеты	Опубликование материалов в открытых источниках
26	Гостиница	Защита персональных данных

Критерии оценки (в баллах):

5 баллов выставляется обучающемуся, если он в полном объеме и правильно выполнил задание (компетенция сформирована на продвинутом уровне);

4 балла выставляется обучающемуся, если он в полном объеме и с незначительными замечаниями выполнил задание (компетенция сформирована на повышенном уровне);

3 балла выставляется обучающемуся, если он на базовом уровне, ошибками выполнил задание(компетенция сформирована на базовом уровне).

Задания для творческого рейтинга

Тематика докладов

Индикаторы достижения: УК-1.1.

1 Информационное право и информационная безопасность.

2 Концепция информационной безопасности.

3 Анализ законодательных актов об охране информационных ресурсов открытого доступа.

4 Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

5 Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.

6 Информационная безопасность (по материалам зарубежных источников и литературы).

7 Правовые основы защиты конфиденциальной информации.

8 Экономические основы защиты конфиденциальной информации.

9 Организационные основы защиты конфиденциальной информации.

10 Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.

11 Составление инструкции по обработке и хранению конфиденциальных документов.

12 Направления и методы защиты документов на бумажных носителях.

13 Направления и методы защиты машиночитаемых документов.

14 Архивное хранение конфиденциальных документов.

15 Направления и методы защиты аудио- и визуальных документов.

16 Порядок подбора персонала для работы с конфиденциальной информацией.

17 Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

18 Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

19 Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

20 Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

21 Назначение, виды, структура и технология функционирования системы защиты информации.

22 Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

23 Аналитическая работа по выявлению каналов утечки информации фирмы.

24 Направления и методы защиты профессиональной тайны.

25 Направления и методы защиты служебной тайны.

27 Направления и методы защиты персональных данных о гражданах.

27 Построение и функционирование защищенного документооборота

28. Наиболее распространенные сетевые атаки.

29. Этапы построения системы защиты информации.

30.Перспективные методы аутентификации.

31.Биометрические системы идентификации и аутентификации.

32. Методы резервирования информации.
33. Типы межсетевых экранов и их краткая характеристика.
34. Отечественные антивирусные программные средства, сертифицированные ФСТЭКРоссии.
35. Стеганография и стеганографические методы защиты информации.
36. Средства защиты передаваемых данных в IP-сетях.
37. Стандарт Ipsec.
38. Угрозы и уязвимости беспроводных сетей.
39. Требования к выбору и использованию паролей.
40. Передача пароля по сети в процессе аутентификации.
41. Лицензирование деятельности, связанной с криптографическими средствамизащиты информации.
42. Сертификация криптографических средств защиты информации.
43. Стандартизация криптографических средств защиты информации.
44. Модель контроля целостности Кларка-Вилсона.
45. Цифровая (электронная) подпись, как механизм контроля целостности.
46. Защита от сбоев программно-аппаратной среды.

Критерии оценки (в баллах):

20 баллов выставляется обучающемуся, если он без ошибок подготовил доклад. Содержание и оформление доклада соответствует требованиям в полном объеме. Уровень сформированности компетенций соответствует продвинутому уровню;

19-14 балла выставляется обучающемуся, если он с незначительными замечаниями по содержанию или оформлению подготовил отчет по реферату. Уровень сформированности компетенций соответствует повышенному уровню;

13-10 балла выставляется обучающемуся, если он с ошибками подготовил отчет по реферату. Содержание и оформление реферата соответствует требованиям не менее, чем на 50 процентов. Уровень сформированности компетенций соответствует базовому уровню.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ ВО ВРЕМЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Структура зачетного задания

Наименование оценочного средства	***Максимальное количество баллов***
Вопрос 1	*15*
Вопрос 2	*15*
Практическое задание 1	*10*

Задания, включаемые в зачетное задание

Типовой перечень вопросов к зачету:

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.
28. Что такое информационная безопасность?
29. Перечислите основные угрозы информационной безопасности.
30. Какие существуют модели и методы информационной безопасности?
31. Что такое правовые методы защиты информации?
32. Что такое организационные методы защиты информации?
33. Что такое технические методы защиты информации?

34. Что такое программно-аппаратные методы защиты информации?

35. Что такое криптографические методы защиты информации?

36. Какие главные государственные органы в области обеспечения информационной безопасности?

37. Перечислите виды защищаемой информации.

38. Какие основные законы в области защиты информации в РФ?

39. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности

40. Что такое концепция информационной безопасности?

41. Что такое конфиденциальная информация?

42. Что такое персональные данные?

43. В каких случаях возможно использовать персональные данные без согласия обладателя?

44. Охарактеризуйте биометрические данные как персональные данные.

45. Что такое профессиональная тайна?

46. Что такое режим коммерческой тайны?

47. Что такое государственная тайна?

48. Опишите правовой режим государственной тайны.

49. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?

50. Как связаны международные стандарты и стандарты РФ?

51. Какие основные стандарты РФ в области информационной безопасности существуют?

52. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.

53. Что такое политика безопасности?

54. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

55. Что такое инженерная защита объектов?

56. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

57. Какие виды компьютерных угроз существуют?

58. Что такое брандмауэр?

59. Что такое антивирусная программа?

60. Что такое эвристический алгоритм поиска вирусов?

61. Что такое сигнатурный поиск вирусов?

62. Методы противодействия сниффингу?

63. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?

64. Что такое механизм контроля и разграничения доступа?

65. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?

66. Что такое средства стеганографической защиты информации?

67. Что такое криптография?

68. Какие используются симметричные алгоритмы шифрования?

69. Какие используются ассиметричные алгоритмы шифрования?
70. Что такое криптографическая хеш-функция?
71. Какие используются криптографические хеш-функции?
72. Что такое цифровая подпись?
73. Что такое инфраструктура открытых ключей?
74. Какие российские и международные стандарты на формирование цифровой подписи существуют?
75. Какие основные криптографические протоколы используются в сетях?

Типовые практические задания:

1. 1	Обеспечить кибербезопасность удалённой работы сотрудников во время пандемии Определить уязвимости сервисов для видеоконференций, ненадёжность VPN, человеческий фактор и не всегда квалифицированные сотрудники — со всем этим неизбежно сталкивается каждая компания, вынужденная организовать удалённую работу. Проанализировать ситуацию и рассказать, как свести к минимуму риски и устранить последствия низкого уровня киберграмотности
2.	Настройка аудита в Windows для полноценного SOC-мониторинга Описать настройку политики аудита Windows таким образом, чтобы охват мониторинга SOC был полноценным. Рассмотреть оптимальный список политик, а также выделить самое необходимое, отсеяв лишнее.
3.	Как проводить контроль продуктивности, защита от мошенничества и утечек данных при удалённой работе сотрудников? Опасность утечки данных и возможность корпоративного мошенничества — неизбежные спутники вынужденной удалённой работы. Рассмотреть, как можно минимизировать риски и справиться с актуальными задачами контроля сотрудников на «удалёнке».
4.	Описать шесть шагов для обеспечения должного уровня безопасности удалённых сотрудников Оперативно переводя сотрудников на дистанционную работу, нужно учесть сопряжённые с этим сложности и не забыть про попытки киберпреступников использовать уязвимые места. Предложить шесть шагов, которые позволят подойти к этому вопросу подготовленными.
5.	Описать требования ГОСТ 34-й серии в проектах по информационной безопасности Что подразумевает требование «проектировать по ГОСТу», становится ли оно менее обязательным? Что делать, если государственный регулятор не предлагает замену для ГОСТов 34-й серии? Какими стандартами стоит руководствоваться при оформлении проектной документации?
6.	Как выявить атаку злоумышленников в сетевом трафике? Обнаружить действия киберпреступников в корпоративной сети и классифицируем их в соответствии с матрицей MITRE ATT&CK, которая показывает, какие тактики и техники применялись в ходе кибератаки.
7.	Описать Microsoft Security Compliance Toolkit: защита Windows групповыми политиками Рассмотреть подход к информационной безопасности комплексно. Описать

	инструменты, которые закрыли бы все «дыры» и создали новые. Описать эталонные настройки политик безопасности и инструменты для работы с ними.
8.	Описать процесс настройки удаленки для сотрудников: Быстро, Безопасно, Бесплатно Что необходимо для организации удаленной работы сотрудников. Какие существуют множества решений способных помочь в реализации этой цели. интернет-шлюз ИКС. С его помощью можно организовать безопасный доступ к сети компании, защититься от вирусов и настроить веб-фильтрацию.
9.	Как организовать безопасную удалённую работу во время карантина? Описать процесс перехода на удалённую работу, рассмотреть очевидные риски для информационной безопасности: модификация трафика, перехват паролей и конфиденциальных данных, а также взлом маршрутизаторов и перенаправление пользователей на вредоносные сайты. Проанализировать контрмеры; в качестве одного из вариантов рассмотреть использование виртуальной частной сети (Virtual Private Network, VPN).
10.	Как построить криптотуннель по ГОСТу с минимальными затратами? Обеспечение безопасности при помощи средств криптографической защиты информации (СКЗИ) — не очень сложная задача, если все технологические участки находятся на хост-машине. Однако для того чтобы передавать и шифровать информацию одновременно, необходимо построить грамотный технологический процесс программного обеспечения.
11.	Как обеспечить безопасность IoT-устройств? Интернет вещей (Internet of Things) — уже очевидная реальность для бизнес-процессов компаний и корпоративных инфраструктур. Однако, несмотря на огромное количество «умных» устройств, работающих на предприятиях и в промышленных сетях, безопасность IoT зачастую оставляет желать лучшего. Как исправить положение, и рассказать о методах защиты интернета вещей.
12.	Как организовать практику организации безопасного удалённого доступа? Что происходит на рынке безопасного удалённого доступа и как правильно защитить подключение сотрудника к корпоративным ресурсам извне? Как регуляторы влияют на процесс дистанционной работы и нужно ли следить за сотрудником, работающим из дома?
13.	Рассмотреть процесс предотвращения вторжений с помощью межсетевого экрана нового поколения UserGate В составе межсетевого экрана нового поколения UserGate применяется система обнаружения вторжений (СОВ) собственной разработки, созданная внутри компании без использования открытого кода. Сигнатуры системы обнаружения вторжений разрабатываются и верифицируются собственной командой аналитиков центра мониторинга и реагирования UserGate.
14.	Как создать комплексную систему безопасности на основе Fortinet Security Fabric API? Открытый и общедоступный API, предназначенный для интеграции продуктов Fortinet с внешними решениями, позволяет пользователям расширять возможности имеющихся компонентов, а также гибко интегрировать сторонние продукты в единую комплексную среду информационной безопасности предприятия.
15.	Как функционирует межсетевой экран UserGate X1: информационная безопасность в экстремальных физических условиях Корпоративный межсетевой экран UserGate X1 выделяется из линейки продуктов UserGate уникальными физико-техническими характеристиками. Данный программно-аппаратный комплекс (ПАК) эффективен и надёжен в

	самых суровых условиях эксплуатации: на промышленных объектах, открытом воздухе, транспорте, сохраняя при этом все преимущества платформы обеспечения профессиональной киберзащиты UserGate.
16.	Описать процесс исполнения требований российских регуляторов по контролю сотрудников Финансовые организации обязаны соблюдать требования положений Банка России и приказов ФСТЭК России. Поскольку назвать список этих требований маленьким язык не поворачивается, мы решили рассмотреть предписания руководящих документов и предложить свой вариант — как можно решить те или иные проблемы или хотя бы облегчить свою участь.
17.	Как предотвратить слив базы данных суперпользователями? Привилегированные пользователи баз данных нередко становятся объектами атак хакеров или сами, пользуясь расширенными правами, эксплуатируют информацию не только в служебных целях. Существует несколько эффективных способов закрытия этих уязвимостей, среди которых можно выделить установку DLP-системы, разграничение доступа, а также ограничение прав суперпользователей до необходимых и достаточных, но удобнее всего автоматизировать защиту от возможных утечек информации из баз данных с помощью коробочных решений, например СУБД Jatoba от компании
18.	Как правильно заполнить журнал учёта СКЗИ? Практически любая организация обменивается конфиденциальными данными со своими партнёрами и структурными подразделениями. Для того чтобы обеспечить сохранность передаваемой информации, требуются средства криптографической защиты (СКЗИ). Но работа с ними регламентируется инструкцией, которая написана 20 лет назад и уже не отвечает современным реалиям, а некоторые её пункты вызывают сомнения у специалистов.
19.	Как выбрать сервис-провайдера для построения SOC? Спрос на услуги коммерческих центров мониторинга и реагирования на инциденты в области информационной безопасности (Security Operations Center, SOC) растёт прямо пропорционально повышению ИБ-зрелости российского бизнеса. Как следствие, увеличивается число сервисных провайдеров, оказывающих услуги по созданию и сопровождению центров мониторинга и реагирования на инциденты. Выбирать провайдера основываясь на громких обещаниях построить SOC «с нуля» в считаные дни — плохая идея.
20.	Безопасность в одном окне: как оптимизировать реагирование с помощью IRP? Платформа автоматизации реагирования на инциденты в информационной безопасности — Incident Response Platform (IRP) — это относительно новый для нашего рынка инструмент, который позволяет автоматизировать процессы мониторинга и повысить эффективность реагирования на кибератаки. Ниже расскажем о том, как именно IRP помогает специалистам по ИБ и как её подключить.

Показатели и критерии оценивания планируемых результатов освоения компетенций и результатов обучения, шкала оценивания

Шкала оценивания		Формируемые компетенции	Индикатор достижения компетенции	Критерии оценивания	Уровень освоения компетенций
85 – 100 баллов	**«отлично»/ «зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	**УК-1.1**. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	**Знает верно и в полном объеме** основные методы критического анализа и основы системного подхода как общенаучного метода. **Умеет верно и в полном объеме** анализировать задачу, используя основы критического анализа и системного подхода. **Умеет верно и в полном объеме** осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации. **Умеет верно и в полном объеме:** использовать современный инструментарий и интеллектуальные информационно-аналитические системы	**Продвинутый**

70 – 84 баллов	**«хорошо»/ «зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	**УК-1.1**. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	**Знает с незначительными замечаниями** основные методы критического анализа и основы системного подхода как общенаучного метода.	**Повышенный**
				Умеет с незначительными замечаниями анализировать задачу, используя основы критического анализа и системного подхода.	
				Умеет с незначительными замечаниями осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации.	
				Умеет с незначительными замечаниями: использовать современный инструментарий и интеллектуальные информационно-аналитические системы	
50 – 69 баллов	**«удовлетворительно»/ «зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	**УК-1.1**. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	**Знает на базовом уровне с ошибками** основные методы критического анализа и основы системного подхода как общенаучного метода.	**Базовый**
				Умеет с незначительными замечаниями анализировать задачу, используя основы критического анализа и системного подхода.	

				Умеет с незначительными замечаниями осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации. **Умеет с незначительными замечаниями:** использовать современный инструментарий и интеллектуальные информационно-аналитические системы	
менее 50 баллов	**«неудовлетворительно»/ «не зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	**УК-1.1**. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	**Не знает на базовом уровне** основные методы критического анализа и основы системного подхода как общенаучного метода. **Не умеет на базовом уровне** анализировать задачу, используя основы критического анализа и системного подхода. **Не умеет с на базовом уровне** осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации. **Не умеет на базовом уровне:** использовать современный инструментарий и интеллектуальные информационно-аналитические системы	**Компетенции не сформированы**