Приложение 6
к основной профессиональной образовательной программе
по направлению подготовки 09.03.03 «Прикладная информатика»
направленность (профиль) программы «Прикладная информатика в экономике»

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

Краснодарский филиал РЭУ им. Г. В. Плеханова

Факультет экономики, менеджмента и торговли

Кафедра экономики и цифровых технологий

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине Информационная безопасность

Направление подготовки **09.03.03 Прикладная информатика**

Направленность (профиль) программы **Прикладная информатика в экономике**

Уровень высшего образования **Бакалавриат**

Год начала подготовки 2024

Краснодар – 2024 г.

Составитель:

к.т.н., доцент кафедры экономики и цифровых технологий Р.Н. Фролов

Оценочные материалы одобрены на заседании кафедры экономики и цифровых технологий Краснодарского филиала РЭУ им. Г.В. Плеханова протокол № 9 от 14 марта 2024 г.

Оценочные материалы составлены на основе рабочей программы по дисциплине «Информационная безопасность», утвержденной на заседании базовой кафедры Прикладной информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университета имени Г.В. Плеханова» протокол № 10 от 28 апреля 2021 г., разработанной авторами:
Козыревым П.А., ассистент, базовой кафедры Прикладной информатики и информационной безопасности
Креопаловым В.В., к.т.н, доцент кафедры прикладной информатики и информационной безопасности

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине Информационная безопасность

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)***	**Наименование контролируемых разделов и тем**
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Понимает базовые принципы постановки задач и выработки решений	УК-2.1. З-1. Знает основные принципы и концепции в области целеполагания и принятия решений УК-2.1. З-2. Знает методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения УК-2.1. З-3. Знает природу данных, необходимых для решения поставленных задач	**Тема 1.** Стандарты и нормативно-правовые акты в области информационной безопасности. **Тема 2.** Анализ рисков и угроз информационной безопасности. **Тема 3.** Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении.
		УК-2.1. У-1. Умеет системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения УК-2.1. У-2. Умеет критически оценивать информацию о предметной области принятия решений УК-2.1. У-3. Умеет использовать инструментальные средства для разработки и принятия решений	
	УК-2.2. Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.2. З-1. Знает основные методы принятия решений, в том числе в условиях риска и неопределенности УК-2.2. З-2. Знает виды и источники возникновения рисков принятия решений, методы управления ими УК-2.2. З-3. Знает основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области	**Тема 1.** Стандарты и нормативно-правовые акты в области информационной безопасности. **Тема 2.** Анализ рисков и угроз информационной безопасности. **Тема 3.** Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении.
		УК-2.2. У-1. Умеет проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений УК-2.2. У-2. Умеет разрабатывать и оценивать альтернативные решения с учетом рисков УК-2.2. У-3. Умеет выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений	

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2. Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности	ОПК-3.2. З-1. Знает методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем ОПК-3.2. З-2. Знает методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах ОПК-3.2. З-3. Знает нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов ОПК-3.2. З-4. Знает основные методы контроля эффективности обеспечения информационной безопасности информационных систем	**Тема 1.** Стандарты и нормативно-правовые акты в области информационной безопасности. **Тема 2.** Анализ рисков и угроз информационной безопасности. **Тема 3.** Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении.
		ОПК-3.2. У-1. Умеет разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС ОПК-3.2. У-2. Умеет выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС ОПК-3.2. У-3. Умеет анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем ОПК-3.2. У-4. Умеет выполнять работы на стадиях и этапах создания ИС в защищенном исполнении ОПК-3.2. У-5. Умеет составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС	

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Перечень учебных заданий на аудиторных занятиях

Темы практических заданий

Тема 1. Стандарты и нормативно-правовые акты в области информационной безопасности.

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 системы информационной 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.

Тема 2. Анализ рисков и угроз информационной безопасности

Задание .

1. Загрузите ГОСТ Р ИСО/МЭК ТО 27005
2. Ознакомьтесь с Приложениями C, D и E ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант).
4. Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь Приложением C ГОСТа 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 ГОСТа произведите оценку рисков информационной безопасности.
7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Варианты

Вариант – номер по списку в журнале.

Номер варианта	Организация	Метод оценки риска (см. Приложение E ГОСТа)
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

Тема 3. Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении.

Задание.

Разработка частной детализированной политики ОИБ

Цель работы: ознакомление с основными частными политиками ОИБ.

1. 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	Центр 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 отдельныхуниверсальных 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 электронномдокументообороте
20	Отделение налоговой службы	Техническая защита информации
21	Офис нотариуса	Реагирование на инциденты ИБ
22	Бюро перевода (документов)	Проведение служебных расследований
23	Научно проектное 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
27	Праздничное агентство	Программная защита
28	Городской архив	Хранение и доступ к конфиденциальной информации
29	Диспетчерская служба такси	Аппаратная защита
30	Железнодорожная касса	Конфиденциальный документооборот

Критерии оценки (в баллах):

- 16-20 баллов выставляется студенту, если все заданиявыполнены не менее чем на 85-95% и в соответствии с рекомендациями, замечаний и ошибок нет; **он умеет верно и в полном объеме:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.
- 11-15 баллов выставляется студенту, есливсе заданиявыполнены не менее чем на 70-84% и в соответствии с рекомендациями, есть замечания и незначительные ошибки; **он умеет с незначительными замечаниями:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.
- 6-10 баллов выставляется студенту, если все заданиявыполнены не менее чем на 50-69%, некоторые задания не выполнены полностью, есть существенные замечания и ошибки**; он умеет на базовом уровне, с ошибками:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и

этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.

- 0-5 баллов выставляется студенту, если все заданияили не выполнены полностьюили выполнены менее чем на 49%,присутствует множество грубых ошибок**; он не умеет на базовом уровне:**системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.

Задания для текущего контроля

Перечень вопросов для контрольной работы

Индикаторы достижения: УК-2.1., УК-2.2., ОПК-3.2.

Темы контрольных работ

Контрольная работа заключается в подготовке письменных ответов на два вопроса, случайно выбранных студентом из числа представленных вопросов для контрольных работ.

Контрольная работа по теме 2. Анализ рисков и угроз информационной безопасности.

1. Идентификация и оценка активов.
2. Модель угроз.
3. Идентификация уязвимостей.
4. Оценка рисков.
5. Обработка рисков.
6. Модель нарушителя политики безопасности.
7. Типичные угрозы информации и уязвимости корпоративных информационных систем.
8. Анализ ошибок, уничтожение, неавторизованная модификация или нецелевое использование информации в прикладных программах.
9. Криптографические меры и средства контроля и управления.
10. Безопасность системных файлов.
11. Безопасность в процессах разработки и поддержки.
12. Модели информационной безопасности.
13. Виды защищаемой информации.
14. Основные нормативно-правовые акты в области информационной безопасности.

15. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.
16. Ресурсы предприятия, подлежащие защите с точки зрения ИБ.
17. Аспекты ИБ в рамках менеджмента непрерывности бизнеса.

Критерии оценки (в баллах):

- 5 баллов выставляется студенту, если он верно и полно (с обоснованиями и выводами) ответил на все вопросы контрольной работы. **Продвинутый уровень усвоения компетенций.**

- 3-4 балла выставляется студенту, если он частично верно ответил на 2 вопроса контрольной работы, при этом допущены незначительные ошибки, выводы и обоснования частично не верны. **Повышенный уровень усвоения компетенций.**

- 1-2 балла выставляется студенту, если смог верно ответить только на один вопрос, но при ответе допустил существенные ошибки, выводы и обоснования частично не верны или не были сделаны. На остальные вопросы не получен ответ.**Базовый уровень усвоения компетенций.**

- 0 баллов выставляется студенту, если он или не участвовал в написании контрольной работы или смог ответить только на один вопрос и при ответе допустил множественные ошибки, не был сделан вывод и обоснования, или ответил на несколько вопросов, но в каждом из них сделал грубые и существенные ошибки, полностью не усвоил значительную часть материала по темам. **Компетенции не сформированы.**

Контрольная работа по теме 3. Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении.

Вопросы для контрольной работы

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 целью дезорганизации 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. Классификация мер обеспечения безопасности компьютерных систем?
28. Задачи, которые должны решаться системой защиты информации?
29. Основные принципы построения систем защиты АСОИ?
30. Основные механизмы защиты компьютерных систем от проникновения с целью дезорганизации их работы и НСД к информации?
31. Методы обеспечения информационной безопасности РФ?
32. Организационные методы информационной безопасности?
33. Направления защиты информационной системы?
34. Этапы создания системы защиты информации?
35. Основные организационные мероприятия?
36. Средства защиты от несанкционированного доступа?
37. Мандатное управление доступом?
38. Избирательное управление доступом?
39. Управление доступом на основе ролей?
40. Системы анализа и моделирования информационных потоков?
41. Защита информации от побочного электромагнитного излучения и наводок?

Критерии оценки (в баллах):

- 5 баллов выставляется студенту, если он верно и полно (с обоснованиями и выводами) ответил на все вопросы контрольной работы. **Продвинутый уровень усвоения компетенций.**

- 3-4 балла выставляется студенту, если он частично верно ответил на 2 вопроса контрольной работы, при этом допущены незначительные ошибки, выводы и обоснования частично не верны. **Повышенный уровень усвоения компетенций.**

- 1-2 балла выставляется студенту, если смог верно ответить только на один вопрос, но при ответе допустил существенные ошибки, выводы и обоснования частично не верны или не были сделаны. На остальные вопросы не получен ответ. **Базовый уровень усвоения компетенций.**

- 0 баллов выставляется студенту, если он или не участвовал в написании контрольной работы или смог ответить только на один вопрос и при ответе допустил множественные ошибки, не был сделан вывод и обоснования, или ответил на несколько вопросов, но в каждом из них сделал грубые и существенные ошибки, полностью не усвоил значительную часть материала по темам. **Компетенции не сформированы.**

Тестовые задания

Тема 1. Стандарты и нормативно-правовые акты в области информационной безопасности

Вопрос	Вариант ответа «a»	Вариант ответа «b»	Вариант ответа «c»	Вариант ответа «d»
Контрольные функции в области государственной безопасности по вопросам предотвращения несанкционированн	**ФСТЭК РФ**	ФСБ РФ	Управлением «К» МВД РФ	Федеральной службой по надзору в сфере связи, информационных технологий и массовых

ого доступа к информации реализуются:				коммуникаций
Защита информации от несанкционированного доступа - это:	**защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации**	деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств	защита информации с помощью ее криптографического преобразования
Несанкционированный доступ к информации - это:	**доступ к информации ресурсам информационной системы, осуществляемый 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**	неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации	неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных	изменение, уничтожение или копирование информации (ресурсов информационной системы), осуществляемое с нарушением установленных прав и (или) правил
Средства контроля и управления доступом - это:	**механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные**	совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью	аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку информации со	аппаратное устройство в составе средств управления СКУД

	средства, обеспечивающие реализацию контроля и управления доступом		считывателей, проведение идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации	
Дискреционное управление доступом - это	**разграничение доступа между поименованными субъектами и объектами; субъект с определенным правом доступа может передать это право любому другому субъекту**	концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам	совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа	разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности
Целостность - это:	**состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право**	состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно	обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее	совокупность свойств служебной информации, обусловливающих ее пригодность удовлетворять определенные потребности в соответствии с ее назначением
Криптографическое средство защиты информации - это:	**средство защиты информации, реализующее алгоритмы криптографического преобразования информации**	техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации	программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности	программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа

Электронная цифровая подпись - это:	**строка бит, полученная в результате процесса формирования подписи**	строка бит, являющаяся выходным результатом хэш-функции	строка бит произвольной конечной длины	строка бит, формируемая из цифровой подписи и произвольного текстового поля
Ключ подписи - это:	**элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи**	элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи	элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам	набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения
Аккредитация удостоверяющего центра - это:	**признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона**	получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата	передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу	процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки подписи и параметры схемы ЭЦП, результатом которого является заключение о правильности или ошибочности цифровой подписи
Средства электронной подписи - это:	**шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи**	программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра	средство защиты информации, реализующее алгоритмы криптографического преобразования информации	техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации

Принципом использования электронной подписи не является принцип:	**возможность использования участниками электронного взаимодействия по своему усмотрению любых информационных систем, позволяющих выполнить требования федеральных законов или принимаемых в соответствии с ними нормативных правовых актов**	право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия	возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей	недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе
Видом электронной подписи не является:	**простая квалифицированная электронная подпись**	простая электронная подпись	усиленная неквалифицированная электронная подпись	усиленная квалифицированная электронная подпись
Обязанностью участников электронного взаимодействия при использовании усиленных электронных подписей не является:	**использовать усиленную электронную подпись для подписания электронных документов, содержащих сведения, составляющие государственную тайну**	обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия	не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена	уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении

Средства электронной подписи не позволяют:	**создавать сертификаты ключей проверки электронных подписей**	установить факт изменения подписанного электронного документа после момента его подписания	обеспечить практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки	создать электронную подпись в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами электронной подписи
Какими свойствами обладает сертификат открытого ключа?	**каждый пользователь, имеющий доступ к открытому ключу CertificationAuthority, может извлечь открытый ключ, включенный в сертификат**	ни одна сторона, помимо CertificationAuthority, не может изменить сертификат так, чтобы это не было обнаружено	всеми перечисленными выше свойствами	ни одним из перечисленных свойств
Каким способом может осуществляться процедура генерации ключей в ходе создания сертификата открытого ключа?	**CertificationAuthority создает пару ключей. Открытый ключ заносится в сертификат, а парный ему секретный ключ передается пользователю с обеспечением аутентификации пользователя и конфиденциальности передачи ключа**	пользователь сам создает пару ключей. Секретный ключ сохраняется у пользователя, а открытый ключ передается по защищенному каналу в CertificationAuthority	обоими способами указанными выше	ни одним из указанных ьвыше способов
Какие базовые модели сертификации существуют в PKI?	**иерархическая модель, основанная на иерархической цепи сертификатов**	модель кросс-сертификации (подразумевает взаимную сертификацию)	сетевая (гибридная) модель, включающая элементы иерархической и взаимной сертификации	все перечисленные выше

Инфраструктура открытых ключей PKI (PublicKeyInfrastructure) — это:	**набор агентов и правил, предназначенных для управления ключами, политикой безопасности и собственно обменом защищенными сообщениями**	локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи	объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных

Критерии оценки (в баллах):

- **8-10 баллов** выставляется студенту, если даны правильные ответы на 80-100% вопросов;**Продвинутый уровень усвоения компетенций.**

- **5-7 балла** выставляется студенту, если даны правильные ответы на 60-79% вопросов;**Повышенный уровень усвоения компетенций.**

- **2-4 балла** выставляется студенту, если даны правильные ответы на 50-59% вопросов;**Базовый уровень усвоения компетенций.**

- **0-1 балл** выставляется студенту, если даны правильные ответы менее чем на 49% вопросов; **Компетенции не сформированы.**

Задания для творческого рейтинга

Темы рефератов

Индикаторы достижения: УК-1.1. ОПК-1.2, ОПК-2.1., ОПК-2.2

Тематика рефератов

1. Наиболее распространенные сетевые атаки.
2. Этапы построения системы защиты информации.
3. Перспективные методы аутентификации.
4. Биометрические системы идентификации и аутентификации.
5. Методы резервирования информации.
6. Типы межсетевых экранов и их краткая характеристика.
7. Отечественные антивирусные программные средства, сертифицированные ФСТЭК России.
8. Стеганография и стеганографические методы защиты информации.
9. Средства защиты передаваемых данных в IP-сетях.
10. Стандарт Ipsec.
11. Угрозы и уязвимости беспроводных сетей.

12. Требования к выбору и использованию паролей.
13. Передача пароля по сети в процессе аутентификации.
14. Лицензирование деятельности, связанной с криптографическими средствами защиты информации.
15. Сертификация криптографических средств защиты информации.
16. Стандартизация криптографических средств защиты информации.
17. Модель контроля целостности Кларка-Вилсона.
18. Цифровая (электронная) подпись, как механизм контроля целостности.
19. Защита от сбоев программно-аппаратной среды.
20. Порядок подбора персонала для работы с конфиденциальной информацией.
21. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
22. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
23. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
24. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
25. Назначение, виды, структура и технология функционирования системы защиты информации.
26. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
27. Аналитическая работа по выявлению каналов утечки информации фирмы.

Критерии оценки (в баллах):

- 17-20 баллов – выставляется обучающемуся, если тема была раскрыта верно, ясно и достаточно, работа носила самостоятельный характер и обладает оригинальностью, качество оформления отчета соответствует требованиям и при защите обучающийся проявил отличное владение материалом работы и способность аргументировано отвечать на поставленные вопросы по теме работы, а также **студент знает верно и в полном объеме:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем.

- 12-16 балла – выставляется обучающемуся, если тема была раскрыта верно, ясно и достаточно, работа носила самостоятельный характер, но нет оригинальности решения, качество оформления отчета соответствует требованиям и при защите обучающийся проявил хорошее владение материалом работы и способность аргументировано отвечать на поставленные вопросы по теме работы, а также **студент знает с незначительными замечаниями:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду

для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем.

- 8-11 балла – выставляется обучающемуся, если тема была раскрыта, работа носила самостоятельный характер, но нет оригинальности решения, качество оформления отчета в основном соответствует требованиям и при защите обучающийся проявил удовлетворительное владение материалом работы и способность отвечать на большинство поставленных вопросов по теме работы, , а также **студент знает на базовом уровне, с ошибками:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем.

- 0-7 балла – выставляется обучающемуся, если работа была выполнена в соответствии с формальными требованиями и тема была в целом раскрыта, но работа не обладает достаточной глубиной исследования вопроса и не содержит оригинального решения, , а также **студент не знает на базовом уровне:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем.

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

Структура экзаменационного билета

Наименование оценочного средства	*Максимальное количество баллов*
Вопрос 1	*14*
Вопрос 2	*14*
Практическое задание	*12*

Задания, включаемые в экзаменационное задание

Вопросы к экзамену:

1. Необходимость обеспечения безопасности в информационных системах.
2. Меры предупреждения преступлений в сфере компьютерной информации.
3. Прогресс информационных технологий и информационная безопасность.
4. История вредоносных программ.
5. Нормативно-правовые аспекты информационной безопасности.
6. Защита учетной информации коммерческих фирм.
7. Классификация угроз безопасности информационных объектов.
8. Свойства экономической информации, нарушаемые при несанкционированном доступе.
9. Основные виды каналов утечки информации.
10. Исторические аспекты компьютерных преступлений.
11. Умышленные и неумышленные угрозы информационной безопасности.
12. Экономическая информация как объект безопасности.
13. Внешние угрозы информационной безопасности.
14. Перечень сведений, которые не могут составлять коммерческую тайну.
15. Мотивы и цели компьютерных преступлений.
16. Виды тайн и как их сохранить.
17. Статьи уголовного кодекса о компьютерных преступлениях.
18. Причины разглашения конфиденциальной информации.
19. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.
20. Разглашение и утечка информации.
21. Объекты информационной безопасности на предприятии.
22. Стратегия злоумышленника при несанкционированном доступе.
23. Организационные методы обеспечения информационной безопасности.
24. Организация конфиденциального делопроизводства.
25. Физическая защита информационных систем.
26. Структура службы безопасности компании.
27. Программно - технические методы обеспечения информационной безопасности.
28. Теоретические аспекты информационной безопасности экономических систем.
29. Идентификация и аутентификация.
30. Основные понятия информационной безопасности экономических систем.
31. Доктрина информационной безопасности Российской Федерации.
32. Экономическая информация как товар и объект безопасности.

33. Государственное регулирование информационной безопасности в России.
34. Понятия информационных угроз и их виды.
35. Несанкционированный доступ и защита от него.
36. Вредоносные программы.
37. Проблема информационной безопасности в историческом аспекте.
38. Компьютерные преступления и наказания.
39. Предупреждение компьютерных преступлений.
40. Принципы построения системы информационной безопасности.
41. Типы компьютерных вирусов и защита от них.
42. Подходы, принципы, методы и средства обеспечения безопасности.
43. Человеческие факторы, обуславливающие информационные угрозы.
44. Организационно-техническое обеспечение компьютерной безопасности.
45. Способы воздействия угроз на информационный объект.
46. Электронная цифровая подпись и особенности ее применения.
47. Признаки воздействия вирусов на компьютерную систему.
48. Защита информации в Интернете.
49. Фрагментарный и системный подходы к защите информации.
50. Организация системы защиты информации экономических систем.
51. Уголовно-правовая характеристика компьютерных преступлений.
52. Этапы построения системы защиты информации.
53. Субъективная сторона компьютерных преступлений.
54. Политика безопасности.
55. Объективная сторона компьютерных преступлений.
56. Оценка эффективности инвестиций в информационную безопасность.
57. Способы совершения компьютерных преступлений («за хвост», «маскарад» и др.).
58. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).
59. Причины и условия, способствующие совершению компьютерных преступлений.
60. Информационная безопасность электронной коммерции (ЭК).
61. Обеспечение компьютерной безопасности учетной информации.
62. Сущность криптографических методов.
63. Организационно-административные мероприятия обеспечения компьютерной безопасности.
64. Организация конфиденциального делопроизводства.
65. Принципы обеспечения информационную безопасности на основе инженерно-технического обеспечения.
66. Типы и субъекты информационных угроз.

Практические задания к экзамену

1. Британский стандарт BS 7799.
2. Британский стандарт BS 7799 – 1.
3. Британский стандарт BS 7799 – 2.
4. Британский стандарт BS 7799 – 3.
5. Международный стандарт ISO/IEC 17799.
6. Семейство Международных стандартов ISO/IEC 27000.
7. Международный стандарт ISO/IEC 27001.
8. Международный стандарт ISO/IEC 27002.
9. Национальный стандарт ГОСТ Р 50922.
10. Национальный стандарт Р 50.1.053.
11. Национальный стандарт ГОСТ Р 51188.
12. Национальный стандарт ГОСТ Р 51275.

13. Национальный стандарт ГОСТ Р ИСО/МЭК 15408.
14. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-1.
15. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-2.
16. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-3.
17. Национальный стандарт ГОСТ Р ИСО/МЭК 17799.
18. Национальный стандарт ГОСТ Р ИСО/МЭК 27001.
19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
23. Порядок защиты информации в рекламной и выставочной деятельности.
24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

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»**	**УК-2.** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением	**УК-2.1.** Понимает базовые принципы постановки задач и выработки решений. **УК-2.2.** Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.2.** Решает задачи профессиональной деятельности с учетом основных требований	**Знает верно и в полном объеме:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности	**Продвинутый**

		информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	информационной безопасности	в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем. **Умеет верно и в полном объеме:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.	

70 – 84 баллов	**«хорошо»**	**УК-2.** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**УК-2.1.** Понимает базовые принципы постановки задач и выработки решений. **УК-2.2.** Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.2.** Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности	**Знает с незначительными замечаниями:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем. **Умеет с незначительными замечаниями:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков;	**Повышенный**

				выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.	
50 – 69 баллов	**«удовлетворительно»**	**УК-2.** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением	**УК-2.1.** Понимает базовые принципы постановки задач и выработки решений. **УК-2.2.** Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.2.** Решает задачи профессиональной деятельности с учетом основных требований	**Знает на базовом уровне, с ошибками:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики	**Базовый**

		информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	информационной безопасности	информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем. **Умеет на базовом уровне, с ошибками:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.	

менее 50 баллов	**«неудовлетворительно»**	**УК-2.** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**УК-2.1.** Понимает базовые принципы постановки задач и выработки решений. **УК-2.2.** Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.2.** Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности	**Не знает на базовом уровне:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем. **Не умеет на базовом уровне:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения	**Компетенции не сформированы**

				исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.	