Приложение 2 к РПД
Информационная безопасность
39.03.01 Социология
направленность (профиль)
Цифровая и экспертно-аналитическая социология
Форма обучения – очная
Год набора – 2022

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

1. Общие сведения

1.	Кафедра	Экономики и управления
2.	Направление подготовки	39.03.01 Социология
3.	Направленность (профиль)	Цифровая и экспертно-аналитическая социология
4.	Дисциплина (модуль)	Информационная безопасность
5.	Форма обучения	очная
6.	Год набора	2022

2. Перечень компетенций и индикаторов

Компетенция	Индикаторы компетенций
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	**2.1.** Формулирует в рамках поставленной цели совокупность взаимосвязанных задач, обеспечивающих ее достижение. **2.2.** Определяет ожидаемые результаты решения выделенных задач. **2.3.** Проектирует решение конкретной задачи, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений. **2.4.** Публично представляет результаты решения конкретной задачи.

3. Критерии и показатели оценивания компетенций на различных этапах их формирования

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформиро-ванности компетенций
		Знать:	Уметь:	Владеть:	
Тема 1. Информационная безопасность и уровни ее обеспечения.	УК-2	Знание основ классификации угроз информационной безопасности	Умение классифицировать и различать, а также проводить оценку угроз и уязвимостей информационной безопасности	Владение методами определения угроз и уязвимостей информационной безопасности, а также классификации потенциальных рисков	Практическая работа Вопросы итогового теста Доклад Глоссарий
Тема 2. Основные нормативные документы в сфере обеспечения информационной безопасности.	УК-2	Знание критериев оценки обеспечения информационной безопасности в соответствии с действующими нормативно-правовыми документами	Умение анализировать и оценивать информационную безопасность в соответствии с требованиями действующих нормативно-правовых документов	Владение практическими основами применения отечественных и международных стандартов обеспечения информационной безопасности	Практическая работа Вопросы итогового теста
Тема 3. Информационная безопасность вычислительных сетей.	УК-2	Знание базовых положений концепции информационной безопасности	Умение использовать модели и методы обеспечения информационной безопасности в соответствии с единой концепцией обеспечения информационной безопасности	Владеть методами оценки эффективности и рисков в соответствии с концепцией обеспечения информационной безопасности	Практическая работа Вопросы итогового теста

Тема 4 Криптографические методы защиты информации	УК-2	Знание теоретических основ обеспечения информационной безопасности	Умение применять методы анализа и оптимизации построения систем защиты информации	Владение методами оценки угроз и уязвимостей, а также эффективности средств и механизмов защиты	Практическая работа Вопросы итогового теста
Тема 5. Технологии и методы построения защищенных информационных систем	УК-2	Знание основных технологий и методов обеспечения информационной безопасности	Умение применять методы обеспечения информационной безопасности в своей профессиональной деятельности	Владение способами организации построения защищенных систем и управления информационной безопасностью	Практическая работа Вопросы итогового теста

Шкала оценивания в рамках балльно-рейтинговой системы
«не зачтено» - 60 баллов и менее, «зачтено» - 61-100 баллов

4. Критерии и шкалы оценивания

Критерии оценки теста

Процент правильных ответов	До 60	61-70	71-80	81-90	91-100
Количество баллов за решенный тест	10	15	20	30	40

Критерии оценки практической работы

Баллы	Характеристики ответа студента
10	- практическая выполнена полностью, без существенных замечаний.
5	- практическая выполнена полностью, есть существенные замечания.

Критерии оценки кейс-стади задания

Баллы	Характеристики ответа студента
10	- задание выполнено полностью, без существенных замечаний.
5	- задание выполнено полностью, есть существенные замечания.

Критерии оценки выступление студентов с докладом

Баллы	Характеристики ответа студента
10	- студент глубоко и всесторонне усвоил проблему; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет понятиями
8	- студент твердо усвоил тему, грамотно и по существу излагает ее, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой основных понятий
5	- тема раскрыта недостаточно четко и полно, то есть студент освоил проблему, по существу излагает ее, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой понятий
0	- студент не усвоил значительной части проблемы; - допускает существенные ошибки и неточности при рассмотрении ее; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений; - не владеет понятийным аппаратом

Критерии оценивания глоссария

№ п/п		Критерии оценки	Количество баллов
1		аккуратность и грамотность изложения	1
2		работа соответствует по оформлению всем требованиям	1

3		полнота исследования темы	1
4		содержание глоссария соответствует заданной теме	1
5		работа сдана в срок	1
		ИТОГО:	**5 баллов**

5. Типовые контрольные задания и методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

5.1 Типовое тестовое задание

1. Главными целями деятельности по обеспечению ИБ являются:

А. Ликвидация угроз объектам информационной безопасности

Б. Минимизация возможного ущерба

В. Исполнение законодательства в области ИБ

Г. Минимизация производственных издержек

Д. Повышение культуры производства

2. Негативные воздействия на объекты ИБ различают:

А. По степени изменения свойств объекта безопасности

Б. По возможности ликвидации последствий проявления угрозы

В. По величине затрат на предотвращение негативного воздействия

3. Укажите свойства угроз:

А. Избирательность

Б. Массовость

В. Стохастичность

Г. Предсказуемость

Д. Вредоносность

4. Выберите верное утверждение(я): Опасность …

А. Это совокупность факторов и условий, возникающих в процессе взаимодействия различных объектов (их элементов) и способных оказывать негативное воздействие на конкретный объект информационной безопасности

Б. Это состояние, в котором находится объект безопасности вследствие возникновения угрозы этому объекту

В. Свойство объекта взаимодействия или находящихся во взаимодействии элементов объекта безопасности, выступающих в качестве источника угроз

Г. является свойством объекта информационной безопасности и характеризует его способность противостоять проявлению угроз

5. По источнику угрозы ИБ делят на:

А. Внутренние

Б. Локальные

В. Общие

Г. Внешние

Д. Частные

6. По видам объектов безопасности угрозы ИБ делят на:

А. Угрозы собственно информации

Б. Угрозы персоналу объекта защиты

В. Угрозы программному обеспечению

Г. Угрозы правовому обеспечению

Д. Угрозы деятельности по обеспечению информационной безопасности

7. К косвенному ущербу ИБ относится:

А. Реализация украденного «стартапа» конкурентами

Б. Затраты на закупку сканеров отпечатков пальцев для доступа к рабочему месту

В. Найм специалистов по обеспечению ИБ

Г. попадание платного контента предприятия в бесплатные обменные сети

Д. Замедление бизнес-процессов в виду запрета доступа некоторым категориям сотрудников к документам данного процесса и, как следствие, возросшая нагрузка на сотрудников и увеличение фонда оплаты труда

8. ИБ направлена на обеспечение:

А. Целостности данных

Б. Репрезентативности данных

В. Адекватности данных

Г. Конфиденциальности данных

Д. Достоверности данных

Е. Доступности данных

9. Укажите виды классификаций угроз ИБ:

А. По источнику (его местонахождению)

Б. По вероятности реализации

В. По вероятности избежания угрозы ИБ

Г. По размерам наносимого ущерба

Д. По природе происхождения

Е. По природе средств защиты

Ж. По предпосылкам возникновения

З. По видам объектов безопасности

10. К прямому ущербу ИБ относится:

А. Потери из-за реализации «стартапа» компании конкурентами

Б. Затраты на закупку сканеров отпечатков пальцев для доступа к рабочему месту

В. Замедление бизнес-процессов в виду запрета доступа некоторым категориям сотрудников к документам данного бизнес-процесса и, как следствие, возросшая нагрузка на сотрудников и увеличение фонда оплаты труда

Г. Использование конкурентами корпоративного механизма доступа к данным

Д. Проигрыш заявки на гос. закупку в виду утечки сведений по данной заявке

Ключ: 1-А,Б, 2-А,Б, 3-А,Г,Д 4-Б,Г,5-А,Г,6-А,Б,Д,7-Б,В,Д,8-А,Г,Е,9-А,Б,Г,Д,Ж,З 10-А,Г,Д.

5.2 Примерные темы докладов:

1. Информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
2. Классификация угроз информационной безопасности и их сравнительный анализ.
3. Информационная безопасность в современных условиях хозяйствования. Общегосударственные цели, задачи и методы обеспечения информационной безопасности.
4. Понятия о видах вирусов. Классификация вирусов и угрозы для информационной инфраструктуры хозяйствующих субъектов.
5. Вида возможных нарушений информационной безопасности в сфере финансовой деятельности.
6. Отечественные и международные стандарты обеспечения информационной безопасности.
7. Особенности современной нормативно-правовой и методологической базы обеспечения информационной безопасности.
8. Основные нормативные руководящие документы, касающиеся конфиденциальной информации и государственной тайны, нормативно-справочные

документы по обеспечению информационной безопасности применяемые в финансовой деятельности.

9. Общие критерии оценки безопасности информационных систем и технологий ГОСТ 15408, как основа определения требований к обеспечению информационной безопасности.

10. Место информационной безопасности экономических систем в национальной безопасности страны.

11. Цели и задачи обеспечения национальной безопасности. Система целеполагания в структуре государственного и муниципального управления при обеспечении информационной безопасности.

12. Основные положения концепции информационной безопасности. Сравнительная таблица.

13. Государственные информационные ресурсы, подлежащие защите в сфере финансовой деятельности.

14. Взаимосвязь государственных и коммерческих информационных ресурсов (конфиденциальной информации и государственной тайны).

15. Модели безопасности, и их применение.

16. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Оценка системы защиты информации.

17. Оценка эффективности средств и механизмов обеспечения информационной безопасности.

18. Методы анализа способов нарушений информационной безопасности.

19. Программно-аппаратные комплексы криптографической защиты, их характеристики и особенности применения. Сравнительная таблица.

20. Нормативно-правовая база криптографической защиты.

21. ЭЦП и особенности работы в системах государственного и муниципального управления.

5.3. Вопросы к зачету

1. Основные принципы защиты информационных технологий (четыре задачи системы защиты).
2. Виды угроз собственной информации в сфере финансовой деятельности.
3. Меры противодействия угрозам собственной информации.
4. Организационно-технические меры защиты информации посредством: охраны зданий; организации использования оргтехники; контроля за посетителями, клиентами.
5. Организационные меры защиты информации посредством контроля за сотрудниками.
6. Организация защиты конфиденциальных документов.
7. Информационная безопасность при использовании средств связи.
8. Организационно-технические методы получения информации о конкурентах.
9. Понятие «изъяны защиты». Причины существования изъянов защиты.
10. Классификация изъянов защиты (по источнику появления, по этапам внедрения, по размещению в информационной системе).
11. Таксономия причин возникновения изъянов защиты.
12. Понятие политики безопасности.
13. Дискретные модели безопасности.
14. Мандатные модели безопасности.
15. Ролевые модели безопасности.
16. Понятия идентификация, аутентификация. Методы и типы аутентификации.
17. Парольные системы защиты.

18. Понятие шифрования. Виды шифрования, применяемые в информационных системах.
19. Способы контроля целостности данных.
20. Цифровая подпись.
21. Хэш-функция.
22. Компьютерная стеганография.
23. Классификация нарушителей по уровню возможностей.
24. Пароль - как метод защиты информации. Виды паролей. Правила подбора паролей.
25. Классификация мероприятий по защите от несанкционированного доступа.
26. Охарактеризовать область физической безопасности АС.
27. Охарактеризовать область безопасности персонала.
28. Охарактеризовать область безопасности оборудования.
29. Охарактеризовать область безопасности ПО.
30. Межсетевые экраны – как метод защиты информации. Дать определение МЭ.
31. Инспектирование и анализ протоколов - как метод защиты информации.
32. Контроль за действиями пользователя и событиями в сети.
33. Принципы восстановления информации и защиты после аварии.
34. Хранение информации. Сжатие и защита информации при хранении.
35. Современные программные угрозы, методы их обнаружения и предупреждения.
36. Методы обнаружения разрушающих программных средств.
37. Намеренное силовое воздействие по каналу связи - как угроза безопасности АС.