

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ**
Защита информации

Код модуля
1161664(1)

Модуль
Интернет-предпринимательство

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Метелев Дмитрий Александрович	кандидат экономических наук, без ученого звания	Доцент	инноватики и интеллектуальной собственности

Согласовано:

Управление образовательных программ

В.В. Топорищева

Авторы:

- Метелев Дмитрий Александрович, Доцент, инноватики и интеллектуальной собственности

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Защита информации

1.	Объем дисциплины в зачетных единицах	4	
2.	Виды аудиторных занятий	Лекции Практические/семинарские занятия	
3.	Промежуточная аттестация	Экзамен	
4.	Текущая аттестация	Контрольная работа	2
		Домашняя работа	2

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Защита информации

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предьявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)	Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине
1	2	3
ПК-9 -Способен разрабатывать и применять алгоритмы и программные приложения для решения практических задач цифровизации в области профессиональной деятельности	З-1 - Сформулировать основные мероприятия в сфере инновационной деятельности для вывода продукции на новые рынки сбыта П-1 - Разрабатывать бизнес-модель монетизации выпускаемой продукции У-1 - Правильно обосновывать инновационные мероприятия, направленные на повышение удовлетворенности выпускаемой продукции у потребителей	Домашняя работа № 1 Домашняя работа № 2 Контрольная работа № 1 Контрольная работа № 2 Лекции Практические/семинарские занятия Экзамен

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО

**ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ
(ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)**

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.6		
Текущая аттестация на лекциях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>контрольная работа №1</i>	6,2	50
<i>контрольная работа №2</i>	6,6	50
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.4		
Промежуточная аттестация по лекциям – экзамен		
Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.6		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.4		
Текущая аттестация на практических/семинарских занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>домашняя работа №1</i>	6,12	50
<i>домашняя работа №2</i>	6,16	50
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям–нет		
Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено		
Текущая аттестация на лабораторных занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
Промежуточная аттестация по лабораторным занятиям –нет		
Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		

Промежуточная аттестация по онлайн-занятиям –нет
Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	Шкала оценивания		
		Традиционная характеристика уровня		Качественная характеристика уровня
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. Основы информационной безопасности. Основные понятия и определения.
2. Политика государства в области информационной безопасности.
3. Модель угроз безопасности информации.
4. Меры обеспечения защиты информации.
5. Криптографические методы защиты информации.
6. Техническая защита информации.
7. Политика безопасности организации.
8. Системы обнаружения и предотвращения компьютерных атак.
9. Основные стандарты в области информационной безопасности.

Примерные задания

Составление модели угроз безопасности информации организации
Планирование мер обеспечения защиты информации.
Криптографические методы защиты информации. Шифрование файлов. Шифрование операционной системы.
Техническая защита информации. Приборы и устройства криптографической защиты
Применение антивирусов, использование мониторов, анализ трафика.
LMS-платформа – не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа № 1

Примерный перечень тем

1. Составление модели угроз безопасности информации организации

Примерные задания

Определение источников угроз.

Выявление критических объектов информационной системы.

Определение перечня угроз для каждого критического объекта.

Выявление способов реализации угроз.

LMS-платформа – не предусмотрена

5.2.2. Контрольная работа № 2

Примерный перечень тем

1. Криптографические методы защиты информации.

2. Шифрование файлов.

3. Шифрование операционной системы.

Примерные задания

Провести шифрование файла штатными средствами операционной системы

Использование ПО TrueCrypt создание зашифрованного раздела диска

Провести сравнительный анализ методов шифрования и криптостойкости

LMS-платформа – не предусмотрена

5.2.3. Домашняя работа № 1

Примерный перечень тем

1. Основные стандарты в области информационной безопасности.

Примерные задания

Привести примеры стандартов. (не менее 3)

Провести сравнительный анализ.

LMS-платформа – не предусмотрена

5.2.4. Домашняя работа № 2

Примерный перечень тем

1. Планирование мер обеспечения защиты информации.

Примерные задания

- Разработать план мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в организации
- Определить перечень разовых мероприятий
- Определить контролирующие и периодические мероприятия:
- Документирование
- Информирование и обучение персонала
- Физический контроль
- Тестирование работоспособности средств защиты информации
- Контроль программного обеспечения и технических средств ИС
- Пользователи, учетные записи, парольная политика
- Беспроводные каналы передачи данных
- Отказоустойчивость
- LMS-платформа – не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Экзамен

Список примерных вопросов

1. Основные понятия информационной безопасности.
2. Информационные технологии и необходимость ИБ.
3. Система защиты информации и ее структуры.
4. Экономическая информация как товар и объект безопасности.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компании.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.
17. Субъекты и причины совершения компьютерных преступлений.
18. Вредоносные программы, их виды.
19. История компьютерных вирусов и современность.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Государственное регулирование информационной безопасности в РФ.
22. Задачи ИБ в программе «цифровая экономика».
23. Доктрина информационной безопасности России.

24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
 25. Уголовно-правовой контроль над компьютерной преступностью в РФ.
 26. Политика безопасности и ее принципы.
 27. Фрагментарный и системный подход к защите информации.
 28. Методы и средства защиты информации.
 29. Организационное обеспечение ИБ.
 30. Организация конфиденциального делопроизводства.
 31. Организационно-экономическое обеспечение ИБ.
 32. Инженерно-техническое обеспечение компьютерной безопасности.
 33. Организационно-правовой статус службы безопасности.
 34. Защита информации в Интернете.
 35. Электронная почта и ее защита.
 36. Защита от компьютерных вирусов.
 37. Популярные антивирусные программы и их классификация.
 38. Этапы и освоение защиты информации экономических объектов.
 39. Криптографические методы защиты информации.
 40. Оценка эффективности инвестиций в информационную безопасность.
 41. Российские компании в сфере ИБ.
 42. Фирмы, оценивающие работу персонала в компании.
 43. Менеджмент и аудит ИБ на уровне предприятия.
 44. Аудит ИБ автоматизированных банковских систем.
 45. Аудит ИБ электронной коммерции.
 46. Информационная безопасность предпринимательской деятельности.
- LMS-платформа – не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	Контрольно-оценочные мероприятия
Формирование социально-значимых ценностей	целенаправленная работа с информацией для использования в практических целях	Технология повышения коммуникативной компетентности	ПК-9	У-1	Домашняя работа № 1 Домашняя работа № 2 Контрольная работа № 1 Контрольная работа № 2 Лекции Практические/семинарские занятия Экзамен