ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Основы информационной безопасности

Код модуля
1158312

Модуль
Введение в профессиональную деятельность

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Леонтьева Юлия Владимировна	кандидат экономических наук, доцент	Доцент	финансового и налогового менеджмента

Согласовано:

Управление образовательных программ И.Ю. Русакова

Авторы:

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Основы информационной безопасности

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Основы информационной безопасности

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление 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**
ОПК-7 -Способен представлять результаты собственной профессиональной деятельности и представлять результаты исследований в виде аналитических отчетов, научных статей, а также при публичных выступлениях с применением современных средств и ориентируясь на	З-2 - Описать принципы подготовки публичного выступления с применением современных средств в зависимости от потребностей аудитории	Домашняя работа № 1 Домашняя работа № 2 Зачет Коллоквиум Контрольная работа Лекции Практические/семинарские занятия

потребности аудитории		
ОПК-2 -Способен применять методы сбора, анализа и интерпретации данных, прогнозировать явления и процессы, составлять и оформлять документы и отчеты по результатам профессиональной деятельности	З-1 - Кратко изложить основные характеристики методов сбора, анализа, интерпретации данных, в том числе для прогнозирования явлений и процессов, значимых для своей профессиональной области задач П-2 - Проводить, применяя методы, сбор и анализ данных, прогнозирование явлений и процессов, характерных для своей профессиональной области, и представлять их интерпретацию в форме научного доклада (сообщения) У-1 - Определять оптимальные методы для сбора, анализа и интерпретации данных, прогнозирования явлений и процессов в своей профессиональной области	Домашняя работа № 1 Домашняя работа № 2 Зачет Коллоквиум Контрольная работа Лекции Практические/семинарские занятия
УК-11 -Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	Д-2 - Демонстрирует самостоятельность в поиске экономической информации, экономических решений; критическое мышление при оценке экономической ситуации, творческий подход к решению экономических задач У-1 - Критически оценивать информацию о последствиях экономической политики, перспективах экономического роста и развития экономики для принятия обоснованных экономических решений	Домашняя работа № 1 Домашняя работа № 2 Зачет Коллоквиум Контрольная работа Лекции Практические/семинарские занятия

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 – 0.7**

Текущая аттестация на лекциях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
домашняя работа №1	5,8	*35*
домашняя работа №2	5,15	*35*
коллоквиум	5,8	*30*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.3		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	5,17	60
подготовка докладов по темам занятий	5,16	40
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**	**Шкала оценивания**

	обучения (выполненное оценочное задание)	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. Свойства информации как объекта защиты
2. Содержание и анализ исторически сложившихся направлений информационной защиты
3. Принципы, стратегии и модели информационной защиты
4. Информационные и компьютерные преступления
5. Информационные войны и информационное оружие

Примерные задания

Занятия проводятся в форме семинаров с обсуждением вопросов по обозначенной теме

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

Примерный перечень тем

1. Информационная безопасность (тестовые задания)

Примерные задания

1. Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.?

2. К каким мерам защиты относится политика безопасности? а) к административным; б) к законодательным; в) к программно-техническим; г) к процедурным.

3. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу? а) ACL; б) списки полномочий субъектов; в) ат-рибутные схемы.

4. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений? а) целостность; б) апеллируемость; в) доступность; г) конфиденциальность; д) аутентичность.

5. К основным принципам построения системы защиты АИС относятся: а) открытость; б) взаимозаменяемость подсистем защиты; в) минимизация привилегий; г) комплексность; д) простота.

6. Какие из следующих высказываний о модели управления доступом RBAC справедливы? а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей; б) роли упорядочены в иерархию; в) с каждым объектом доступа ассоциировано несколько ролей ; г) для каждой пары «субъект-объект» назначен набор возможных разрешений.

7. Диспетчер доступа... а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа; б) ... использует атрибутные схемы для представления матрицы доступа; в) ... выступает посредником при всех обращениях субъектов к объектам; г) ... фиксирует информацию о попытках доступа в системном журнале;

8. Какие предположения включает неформальная модель нарушителя? а) о возможностях нарушителя; б) о категориях лиц, к которым может принадлежать нарушитель; в) о привычках нарушителя; г) о предыдущих атаках, осуществленных нарушителем; д) об уровне знаний нарушителя.

9. Что представляет собой доктрина информационной безопасности РФ? а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информа-ционной безопасности; б) федеральный закон, регулирующий правоотношения в области информационной безопасности; в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и

этапов; г) сово-купность официальных взглядов на цели, задачи, принципы и основные направления обес-печения информационной безопасности Российской Федерации.

10. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности? а) политика безопасности верхнего уровня; б) политика безопасности среднего уровня; в) политика безопасности нижнего уровня; г) принцип минимизации привилегий; д) защита поддерживающей инфраструктуры.

LMS-платформа − не предусмотрена

5.2.2. Коллоквиум

Примерный перечень тем

1. Необходимость обеспечения безопасности в информационных системах
2. Прогресс информационных технологий и информационная безопасность
3. Нормативно-правовые аспекты информационной безопасности
4. Классификация угроз безопасности информационных объектов
5. Основные виды каналов утечки информации
6. Способы воздействия угроз на информационный объект
7. Признаки воздействия вирусов на компьютерную систему
8. Исторические аспекты компьютерных преступлений
9. Причины разглашения конфиденциальной информации
10. Структура службы безопасности компании

Примерные задания

Коллоквиум предполагает письменные ответы на тематические вопросы. Коллоквиум прово-дится перед выполнением практической работы и позволяет оценить степень готовности студента к ее выполнению.

LMS-платформа − не предусмотрена

5.2.3. Домашняя работа № 1

Примерный перечень тем

1. Формы психологической защиты человека от информационной перегрузки
2. Социально вредная информация в СМИ
3. Вредная и опасная информация в Интернет
4. Формы и методы недобросовестной рекламной деятельности
5. Формы обмана и мошенничества в Интернет
6. Атаки на информационные системы путем перегрузки каналов связи и входных буферов памяти. Использование «протоколов вежливости» для реализации сетевых атак
7. Способы подделки компьютерной информации (денег, документов, доказательств) и программный инструментарий
8. Компьютерное «пиратство» и его формы. Перспективы противодействия незаконному копированию компьютерной информации
9. Формы незаконного использования информации. Законодательные меры против незаконного использования информации
10. Формы и методы диверсионно-террористической деятельности с использованием современных информационных технологий

Примерные задания

Домашняя работа выполняется в виде подготовки устного сообщения по выбранной теме с презентацией его результатов в рамках практических занятий в виде слайдов.

LMS-платформа − не предусмотрена

5.2.4. Домашняя работа № 2

Примерный перечень тем

1. Виды и формы применения информационно-технологического оружия
2. Доктрина информационной безопасности России и реальности ее осуществления
3. Анализ способов информационного воздействия и форм информационной защиты, отраженных в сказках, сказаниях, былинах и мифах
4. Государственная система защиты граждан и общества от опасной информации (законодательство и практика)
5. Вопросы информационной безопасности в теории военного искусства
6. Вопросы информационной безопасности в политике и дипломатии
7. Формы и методы выживания биологических особей и возможности их применения при защите информации
8. Стратегия пассивной информационной защиты
9. Стратегия уничтожения источника угроз в сфере информационной защиты
10. Стратегия обмана и ее использование в сфере информационной защиты
11. Модель комплексной информационной защиты и ее элементы
12. Модель информационной защиты каналов связи
13. Угрозы скрытого информационного воздействия на пользователей Интернет
14. Формы и методы защиты признаковой информации
15. Информация как ценность и объект преступных посягательств
16. Угрозы конфиденциальности и формы их реализации
17. Модель информационного нарушителя, посягающего на конфиденциальную информацию методами несанкционированного доступа
18. Задачи информационной защиты в финансовой сфере
19. Задачи информационной защиты в сфере предоставление услуг связи
20. Традиционные направления информационной защиты и пути их интеграции

Примерные задания

Домашняя работа выполняется в виде подготовки устного сообщения по выбранной теме с презентацией его результатов в рамках практических занятий в виде слайдов.

LMS-платформа − не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

1. Основные понятия информационной безопасности
2. Угрозы информационной безопасности
3. Каналы утечки информации
4. Неформальная модель нарушителя
5. Информационная безопасность на уровне государства
6. Задачи системы информационной безопасности

7. Меры противодействия угрозам безопасности
8. Основные принципы построения систем защиты АИС
9. Понятие и назначение модели безопасности
10. Основные понятия криптографии
11. Шифрование
12. Современные алгоритмы симметричного шифрования
13. Режимы функционирования блочных шифров
14. Шифрование с открытым ключом. ЭЦП
15. Алгоритмы шифрования с открытым ключом
16. Электронная цифровая подпись
17. Российский стандарт электронной цифровой подписи
18. Российский стандарт хэширования
19. Понятие криптографического протокола
20. Роль парольной защиты в обеспечении безопасности АИС
21. Способы атаки на пароль. Обеспечение безопасности пароля
22. Общие сведения о компьютерных вирусах. Классификация вирусов
23. Средства защиты сети
24. Криминологическая характеристика компьютерных преступлений
25. Объект и предмет преступлений в сфере компьютерной информации.

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**
Воспитание навыков жизнедеятельности в условиях глобальных вызовов и неопределенностей	целенаправленная работа с информацией для использования в практических целях	Технология самостоятельной работы	УК-11	У-1 Д-2	Домашняя работа № 1 Домашняя работа № 2 Зачет Коллоквиум