СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Экономический***
Кафедра ***Бухгалтерского учета и аудита***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Информационная безопасность экономических систем***

Блок Б1, часть, формируемая участниками образовательных отношений, Б1.В.14
цикл дисциплины и его часть (обязательная часть или часть, формируемая участниками образовательных отношений)

Специальность

38.05.01	***Экономическая безопасность***
код	наименование специальности

Программа

Экономико-правовое обеспечение экономической безопасности

Форма обучения

Очная

Для поступивших на обучение в
2023 г.

Разработчик (составитель)
кандидат педагогических наук, доцент
Рафикова В. М.
ученая степень, должность, ФИО

Стерлитамак 2023

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3	4				5
			неуд.	удовл.	хорошо	отлично	
ПК-1. Способен разработать интегрированную систему управления рисками	ПК-1.1. Применяет современные информационные системы и технологии управления рисками	Обучающийся должен: Знать -источники возникновения информационных угроз; -каналы утечки информации; -направления и средства защиты информации; -принципы национальной безопасности. Уметь - применять правовые, организационные, технические и программные средства защиты	Отсутствуют знания, умения и навыки	Имеет представление о -источниках возникновения информационных угроз; -каналах утечки информации; -направлениях и средствах защиты информации; -принципах национальной безопасности. Умеет - применять правовые, организационные, технические и программные средства защиты	Знает -источники возникновения информационных угроз; -каналы утечки информации; -направления и средства защиты информации; -принципы национальной безопасности. Умеет - применять правовые, организационные, технические и программные средства защиты информации; - выявлять	Отлично знает -источники возникновения информационных угроз; -каналы утечки информации; -направления и средства защиты информации; -принципы национальной безопасности. Умеет - применять правовые, организационные, технические и программные средства защиты информации; - выявлять	Тестирование Подготовка докладов

		информации; - выявлять потенциальные каналы утечки информации и определять их характеристики; - разрабатывать и обосновывать варианты эффективных управленческих решений в области управления рисками. Владеть - навыками противодействия утечке компьютерной информации; - навыками использования электронной цифровой подписи; - навыками проведения аудита локальной политики		информации; - выявлять потенциальные каналы утечки информации и определять их характеристики. Владеет начальными - навыками противодействия утечке компьютерной информации; - навыками использования электронной цифровой подписи	потенциальные каналы утечки информации и определять их характеристики; - разрабатывать и обосновывать варианты эффективных управленческих решений в области управления рисками. Владеет - навыками противодействия утечке компьютерной информации; - навыками использования электронной цифровой подписи; - навыками проведения аудита локальной политики безопасности, аудита доступа к	потенциальные каналы утечки информации и определять их характеристики; - разрабатывать и обосновывать варианты эффективных управленческих решений в области управления рисками. Владеет - навыками противодействия утечке компьютерной информации; - навыками использования электронной цифровой подписи; - навыками проведения аудита локальной политики безопасности, аудита доступа к	

		безопасности, аудита доступа к объектам - навыками профессиональной аргументации при разборе стандартных ситуаций в сфере управления рисками.			объектам.	объектам - навыками профессиональной аргументации при разборе стандартных ситуаций в сфере управления рисками.	
	ПК-1.2. Использует программное обеспечение для работы с информацией	Обучающийся должен: Знать - основные функциональные возможности современных программных средств. Уметь - использовать основные функциональные возможности современных программных средств. Владеть - навыками	Отсутствуют знания, умения и навыки	Имеет общее представление об основных функциональных возможности современных программных средств. Может пересказать основные функциональные возможности современных программных средств. Владеет начальными - навыками	Знает основные функциональные возможности современных программных средств. Умеет - использовать основные функциональные возможности современных программных средств. Владеет - навыками использования основных функциональных	Отлично знает - основные функциональные возможности современных программных средств. Умеет - использовать основные функциональные возможности современных программных средств. Владеет - навыками использования основных	Тестирование Подготовка докладов

		использования основных функциональных возможностей современных программных средств поддержки профессиональной деятельности		использования основных функциональных возможностей современных программных средств поддержки профессиональной деятельности	возможностей современных программных средств поддержки профессиональной деятельности	функциональных возможностей современных программных средств поддержки профессиональной деятельности	
	ПК-1.3. Осуществляет мониторинг наиболее критичных рисков, их динамики и вырабатывает рекомендаций по дальнейшему развитию системы управления рисками	Обучающийся должен: Знать - порядок проведения мониторинга информационной безопасности объектов и систем Уметь - проводить мониторинг информационной безопасности объектов Владеть - навыками проведения мониторинга информационно	Отсутствуют знания, умения и навыки	Имеет общее представление о порядке проведения мониторинга информационной безопасности объектов и систем Может пересказать процедуру мониторинга информационной безопасности объектов Владеет начальными навыками проведения мониторинга	Знает порядок проведения мониторинга информационной безопасности объектов и систем Умеет - проводить мониторинг информационной безопасности объектов Владеет - навыками проведения мониторинга информационной безопасности объектов и систем на	Отлично знает порядок проведения мониторинга информационной безопасности объектов и систем Умеет - проводить мониторинг информационной безопасности объектов Владеет - навыками проведения мониторинга информационной безопасности объектов и	Тестирование Подготовка докладов

		й безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	соответствие требованиям стандартов в области информационной безопасности	систем на соответствие требованиям стандартов в области информационной безопасности	

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)

Перечень тестовых заданий для оценки уровня сформированности компетенции ПК-1 на этапе «Знания»:

Тестовые задания к разделу 1

1. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется
1. актуальностью информации
2. доступностью
3. качеством информации
4. целостностью

2. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев
1. C
2. A
3. B
4. D

3. Организационные требования к системе защиты
1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические

4. Основу политики безопасности составляет
1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи

5. Соответствие средств безопасности решаемым задачам характеризует
1. эффективность
2. корректность
3. адекватность
4. унификация

6. С точки зрения ФСТЭК основной задачей средств безопасности является обеспечение сохранности информации
1. защиты от НСД
2. простоты реализации
3. надежности функционирования

7. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне
1. E5
2. E7
3. E4
4. E6

8. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это
1. аудит
2. аутентификация
3. авторизация
4. идентификация

9. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь
1. наиболее важные субъекты
2. наиболее важные объекты

3. все субъекты
4. все объекты
10. Соответствие средств безопасности решаемым задачам характеризует
1. эффективность
2. корректность
3. адекватность
4. унификация
11. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется
1. системой защиты
2. стандартом безопасности
3. профилем безопасности
4. профилем защиты
12. Для решения проблемы правильности выбора и надежности функционирования средств защиты в «европейских критериях» вводится понятие
1. унификации средств защиты
2. надежности защиты информации
3. адекватности средств защиты
4. оптимизации средств защиты

Перечень тестовых заданий для оценки уровня сформированности компетенции ПК-1 на этапе «Умения»:
Тестовые задания к разделу 2
1. Организационные требования к системе защиты
1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические
2. Основу политики безопасности составляет
1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи
3. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности
1. Лендвера
2. С полным перекрытием
3. Белла-ЛаПадула
4. На основе анализа угроз
4. Из перечисленного услуга защиты целостности доступна на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом
1. 1, 2, 5
2. 1, 3, 5
3. 1, 2, 3
4. 4, 5, 6
5. Присвоение субъектам и объектам доступа уникального номера, шифра, ключа и т.п. с целью получения доступа к информации — это
1. идентификация
2. аудит
3. авторизация
4. аутентификация
6. Из перечисленного типами услуг аутентификации являются: 1) идентификация; 2)

достоверность происхождения данных; 3) достоверность объектов коммуникации; 4) причастность;
1. 3, 4
2. 1, 4
3. 2, 3
4. 1, 2
7. Как предотвращением неавторизованного использования ресурсов определена услуга защиты
1. аутентификация
2. причастность
3. контроль доступа
4. целостность
8. Пользовательское управление данными реализуется на уровне модели взаимодействия открытых систем представления данных
1. канальном
2. сеансовом
3. прикладном

Перечень тестовых заданий для оценки уровня сформированности компетенции ПК-1 на этапе «Знания»:

Тестовые задания к разделу 3

1. Наукой, изучающей математические методы защиты информации путем ее преобразования, является
1. криптоанализ
2. криптология
3. стеганография
4. криптография
2. Конечное множество используемых для кодирования информации знаков называется
1. шифром
2. кодом
3. алфавитом
4. ключом
3. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет
1. криптология
2. стеганография
3. криптоанализ
4. криптография
4. Обеспечением скрытности информации в информационных массивах занимается
1. криптография
2. криптоанализ
3. криптология
4. стеганография
5. Два ключа используются в криптосистемах
1. с открытым ключом
2. с закрытым ключом
3. двойного шифрования
4. симметричных
6. Главным параметром криптосистемы является показатель
1. безошибочности шифрования
2. скорости шифрования
3. криптостойкости
4. надежности функционирования

7. Длина исходного ключа в ГОСТ 28147-89 (бит)
1. 128
2. 256
3. 64
8. Основной целью системы брандмауэра является управление доступом
1. к архивам
2. внутри защищаемой сети
3. к секретной информации
4. к защищаемой сети
9. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки адресов отправителя и получателя
1. содержания сообщений
2. электронной подписи
3. структуры данных
10. Из перечисленного система брандмауэра может быть: 1) репитором; 2) маршрутизатором; 3) ПК; 4) хостом; 5) ресивером
1. 3, 4, 5
2. 2, 3, 4
3. 1, 4, 5
4. 1, 2, 3

Перечень тем для подготовки докладов для оценки уровня сформированности компетенции ПК-1 на этапе «Владения»:

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.

Вопросы к зачету

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2. Доступность, целостность, конфиденциальность.
3. Компьютерное преступление, жизненный цикл информационных систем.
4. Сложные системы. Структурный подход.
5. Основные определения и критерии классификации угроз.
6. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
7. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
8. Российское законодательство в области информационной безопасности.
9. Зарубежное законодательство в области информационной безопасности.
10. Стандарты и спецификации в области информационной безопасности.
11. Основные понятия, политика безопасности.
12. Жизненный цикл информационной системы.
13. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
14. Основные классы мер процедурного уровня.
15. Управление персоналом. Физическая защита.
16. Поддержание работоспособности.
17. Реагирование на нарушения режима безопасности.
18. Планирование восстановительных работ.
19. Основные понятия программно-технического уровня. Архитектурная безопасность.
20. Экранирование. Анализ защищённости.
21. Отказоустойчивость. Безопасное восстановление.
22. Основные понятия криптографии.
24. Парольная аутентификация. Одноразовые пароли.
25. Идентификация/аутентификация с помощью биометрических данных.
26. Управление доступом. Ролевое управление доступом.
27. Активный аудит. Шифрование.
28. Симметричный метод шифрования.
29. Асимметричный метод шифрования.
30. Секретный и открытый ключ.
31. Криптография. Контроль целостности
32. Цифровые сертификаты.
33. Электронная цифровая подпись.
34. Экранирование. Фильтрация. Межсетевые экраны.

35. Классификация межсетевых экранов.
36. Архитектурная безопасность.
37. Транспортное экранирование. Анализ защищенности.
38. Сетевой сканер. Антивирусная защита.

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Раздел 1				
Текущий контроль				
1. Устный опрос	5	3	0	15
2. Доклады	1	5	0	5
Рубежный контроль				
1. Тестирование	15	1	0	15
Раздел 2				
Текущий контроль				
1. Устный опрос	5	3	0	15
2. Доклады	1	5	0	5
Рубежный контроль				
1. Тестирование	15	1	0	15
Поощрительные баллы				**10**
1. Студенческая олимпиада				
2. Публикация статей				
3. Участие в конференции				
4. Активная работа на аудиторных занятиях				
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			**0**	**–6**
2. Посещение практических занятий			**0**	**–10**
Итоговый контроль				
Зачет с оценкой	30		0	30

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл = k × Максимальный балл,

где k = 0,2 при уровне освоения «неудовлетворительно», k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов УУНиТ:
На дифференцированном зачете выставляется оценка:
• отлично - при накоплении от 80 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
• хорошо - при накоплении от 60 до 79 рейтинговых баллов,
• удовлетворительно - при накоплении от 45 до 59 рейтинговых баллов,
• неудовлетворительно - при накоплении менее 45 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.