СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

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

Оценочные материалы по дисциплине (модулю)

дисциплина ***Информационная безопасность в цифровой экономике***

Блок Б1, вариативная часть, Б1.В.ДВ.03.01
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

38.03.01 ***Экономика***
код наименование направления

Программа

Бухгалтерский учет, анализ и аудит

Форма обучения

Заочная

Для поступивших на обучение в
2020 г.

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

Стерлитамак 2022

1. Перечень компетенций с указанием этапов их формирования и описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Формируемая компетенция (с указанием кода)	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3				4
		неуд.	удовл.	хорошо	отлично	
Способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-8)	1 этап: Знания	Отсутствие навыков	Имеет первоначальные навыки - применения в профессиональной деятельности автоматизированные рабочие места - проведения информационно-поисковой работы с последующим использованием данных при решении профессиональных задач.	Обладает навыками - применять в профессиональной деятельности автоматизированные рабочие места - проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	Умеет использовать в профессиональной деятельности автоматизированные рабочие места информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	Выполнение практических заданий
	2 этап: Умения	Отсутствие умений	В основном умеет -использовать автоматизированные информационные системы -использовать автоматизированные	Умеет использовать -использовать автоматизированные информационные системы -использовать автоматизированные	Умеет производить -использовать автоматизированные информационные системы -использовать автоматизированные	Выполнение практических заданий

			рабочие места	рабочие места	рабочие места	
	3 этап: Владения (навыки / опыт деятельности)	Отсутствие знаний	Имеет представление автоматизированных рабочих мест; -современных информационных технологии для поиска и обработки экономической информации.	Имеет хорошие предметные знания автоматизированных рабочих мест; -современных информационных технологии для поиска и обработки экономической информации.	имеет отличные знания автоматизированных рабочих мест; -современных информационных технологии для поиска и обработки экономической информации.	Письменная контрольная работа. Тестовые задания
Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1)	1 этап: Знания	Отсутствие знаний	Имеет представление о –источниках возникновения информационных угроз, -каналах утечки информации, -направлениях и средствах защиты информации, -принципах национальной безопасности, -исследования, ведущиеся в области, информационной безопасности,	Имеет хорошие предметные знания - источников возникновения информационных угроз, -каналов утечки информации, -направления и средства защиты информации, -принципов национальной безопасности, -исследования, ведущиеся в области, информационной безопасности,	имеет отличные знания источников возникновения информационных угроз, -каналов утечки информации, -направления и средства защиты информации, -принципов национальной безопасности, -исследования, ведущиеся в области, информационной безопасности,	Письменная контрольная работа. Тестовые задания

	2 этап: Умения	Отсутствие умений	В основном умеет использовать - примение правовых, организационных, технических, - выявлять потенциальные каналы утечки информации и определять их характеристики, - разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности, - систематизировать и обобщать информацию, готовить обзоры по вопросам информационной безопасности	Умеет использовать - применение правовых, организационных, технических, - выявлять потенциальные каналы утечки информации и определять их характеристики, - разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности, - систематизировать и обобщать информацию, готовить обзоры по вопросам информационной безопасности	Умеет - применять правовые, организационные, технически, - выявлять потенциальные каналы утечки информации и определять их характеристики, - разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности, - систематизировать и обобщать информацию, готовить обзоры по вопросам информационной безопасности	Выполнение практических заданий
	3 этап: Владения (навыки / опыт деятельности)	Отсутствие навыков	Имеет первоначальные навыки противодействия утечке компьютерной	Обладает - навыками противодействия утечке компьютерной информации	Умеет использовать - навыки противодействия утечке компьютерной информации	Выполнение практических заданий

			информации - навыки использования электронной цифровой подписи, - навыки проведения аудита локальной политики безопасности, аудита доступа к объектам, - специальной терминологией, применяемой в процессе защиты информации, - навыки профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности	- навыками использования электронной цифровой подписи, - навыками проведения аудита локальной политики безопасности, аудита доступа к объектам, - специальной терминологией, применяемой в процессе защиты информации, - навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности	- навыки использования электронной цифровой подписи, - навыки проведения аудита локальной политики безопасности, аудита доступа к объектам, - специальной терминологией, применяемой в процессе защиты информации, - навыки профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности	

2. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Темы контрольных работ

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.

Тестовые задания к разделу 1(ОПК-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
20
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

Тестовые задания к разделу 2 (ПК-8)

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

Тестовые задания к разделу 3 (ПК-8; ОПК-1)

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

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 знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Рейтинг - план дисциплины

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий	Баллы	
			Минимальный	Максимальный
Раздел 1.				
Текущий контроль			**0**	**20**
Аудиторная работа - выполнение практических работ	3	5	0	15
Контроль самостоятельной работы	2,5	2	0	5
Рубежный контроль			**0**	**25**
Контрольная работа №1	15	1	0	15
Тестирование	10	1	0	10
Раздел 2.				
Текущий контроль			**0**	**30**

Аудиторная работа - выполнение практических работ	2	11	0	22
Контроль самостоятельной работы	2	4	0	8
Рубежный контроль			**0**	**25**
Контрольная работа №2	15	1	0	15
Тестирование	10	1	0	10
		Итого:	**0**	**100**
Поощрительные баллы			**0**	**10**
Участие в конференции				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических занятий			0	-10

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 БашГУ:

На зачете выставляется оценка:

• зачтено - при накоплении от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

• не зачтено - при накоплении от 0 до 59 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.