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

Факультет ***Математики и информационных технологий***
Кафедра ***Прикладной информатики и программирования***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Информационная безопасность предприятия***

Блок Б1, базовая часть, Б1.Б.33
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

Разработчик (составитель)
к.ф.-м.н, заведующий кафедрой
Хасанов М. К.
ученая степень, должность, ФИО

Стерлитамак 2023

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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	1 этап: Знания	Отсутствие знаний об информационных ресурсах, подлежащих защите, угрозах безопасности информации и возможных путях их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Неполные представления об информационных ресурсах, подлежащих защите, угрозах безопасности информации и возможных путях их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Сформированные, но содержащие отдельные пробелы представления об информационных ресурсах, подлежащих защите, угрозах безопасности информации и возможных путях их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Сформированные систематические представления об информационных ресурсах, подлежащих защите, угрозах безопасности информации и возможных путях их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Устный опрос
	2 этап: Умения	Отсутствие навыков	В целом успешное, но непоследовательное	В целом успешное, но содержащее отдельные пробелы	Успешное и последовательное владение навыками	Тесты

			владение навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	владения навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	3 этап: Владения (навыки / опыт деятельности)	Отсутствие умений	В целом успешное, но не систематическое умение определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания	В целом успешное, но содержащее отдельные пробелы в умении определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа	Сформированное умение определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных	Тесты

			информационных процессов и особенностей функционирования объекта защиты	структуры и содержания информационных процессов и особенностей функционирования объекта защиты	процессов и особенностей функционирования объекта защиты	
Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)	1 этап: Знания	Отсутствие знаний	Неполные представления об особенностях организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации	Сформированные, но содержащие отдельные пробелы представления об особенностях организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации	Сформированные систематические представления об особенностях организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации	Устный опрос
	2 этап: Умения	Отсутствие умений	В целом успешное, но не систематическое умение принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	В целом успешное, но содержащее отдельные пробелы в умении принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Сформированное умение принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Тесты

	3 этап: Владения (навыки / опыт деятельности)	Отсутствие навыков	В целом успешное, но непоследовательное владение навыками принятия участия в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	В целом успешное, но содержащее отдельные пробелы владения навыками принятия участия в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Успешное и последовательное владение навыками принятия участия в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Тесты

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

Вопросы для устного опроса (ОПК-7 Знания):

1. Информация как объект правового регулирования. Источники права в области информационной безопасности.
2.Меры защиты информации: законодательного, административного, процедурного, программно-технического уровней.
3.Законодательство РФ в области информационной безопасности.
4.Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
5.Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
6. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
7. Основные цели и задачи обеспечения информационной безопасности в компьютерных системах.
8. Методы несанкционированного доступа к информации в компьютерных системах.
9. Фундаментальные понятия описания моделей и механизмов безопасности.
10. Характеристика парольных систем для защиты компьютерной информации от несанкционированного доступа.
13. Перечислить и дать характеристику базовым признакам возможных угроз безопасности информации в компьютерных системах.
14. Основные методы реализации угроз информационной безопасности АС.
15.Дать характеристику основным принципам обеспечения информационной безопасности в АС.
16.Каналы утечки информации, выделяемые применительно к компьютерной системе.
17. Необходимые требования и критерии стандартов информационной безопасности компьютерных систем.
18. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
19.Критериоценкибезопасностикомпьютерныхсистем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
20.Виды гарантированности, рассматриваемые в «Оранжевой книге».

Вопросы для устного опроса (ПК-5 Знания):

1.Какие уровни доверия и классы безопасности определены в «Оранжевой книге»?
2.Виды требований безопасности, которые содержат «Общие критерии».
3. Параметры объекта оценки в «Общих критериях» и параметр, характеризующие угрозы.
4. Иерархия, введенная в «Общих критериях» для структурирования пространства требований.
5.Классы функциональных требований «Общих критериев».
6.Дать анализ основным недостаткам «Общих критериев».
7.Задачи средств криптографической защиты информации (СКЗИ) и особенности их использования.
8. Криптосистема DES.
9. Криптосистема RSA.
10.Криптографическиепротоколы. Проблемы криптографических протоколов. Электронная цифровая подпись. Свойства электронной цифровой подписи. Схема генерации и проверки электронной цифровой подписи.
11. Перечислить и дать характеристику основным требованиям к СКЗИ.
12.Способыи особенности реализации криптографических систем.

13. Определение: «цифровая подпись».Классы формирования цифровой подписи.
14. Основные направления обеспечения информационной безопасности в компьютерных системах.
15. Показатели защищенности АС от НСД.
16. Понятие «анализа рисков» в компьютерной системе.
17.Модель вероятного злоумышленника, анализ его возможностей.
18.Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.

Тестовые задания (ОПК-7 Умения):
1.Под Информационной безопасностью понимают:
а) защиту от несанкционированного доступа;
б) защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера;
с) защиту информации от компьютерных вирусов.
2. Аутентификация - это:
а) проверка количества переданной и принятой информации;
б) нахождение файлов, которые изменены в информационной системе несанкционированно;
в) проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа);
г) определение файлов, из которых удалена служебная информация;
3. Физические средства защиты информации - это:
1) средства, которые реализуются в виде автономных устройств и систем;
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;
3) это программы, предназначенные для выполнения функций, связанных с защитой информации;
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств;
4.Основная причина потерь информации, связана с:
1)глобальным хищением информации;
2)появлением Интернета;
3) с недостаточной образованностью в области безопасности.
5. Технические средства защиты информации- это:
1) средства, которые реализуются в виде автономных устройств и систем;
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;
3) это программы, предназначенные для выполнения функций, связанных с защитой информации;
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств;
6.Несанкционированный доступ - это:
1) доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;
2) создание резервных копий в организации;
3) правила и положения, выработанные в организации для обхода парольной защиты;
4) вход в систему без согласования с руководителем организации;
5) удаление не нужной информации.

Тестовые задания (ПК-5 Умения):
1.Криптография -это:
1) математические методы скрытия информации;

2) кодирование информации;
3) математические методы защиты информации.
2.Криптоанализ-это:
1) дешифрование информации без знания ключа;
2) восстановление исходного сообщения, исходя только из шифртекста;
3) разработка атак на засекреченную информацию.
3.Ключ шифрования - это:
1) шифр;
2) пароль;
3) конкретное криптографическое преобразование, обеспечивающее выбор одного преобразования из семейства преобразований открытого текста в зашифрованный.
4.Один и тот же ключ для шифрования и расшифрования используется:
1) в симметричных криптосистемах;
2) в асимметричных криптосистемах;
3) при хэшировании.
5.Целостность информации - это:
1) свойство информации, заключающееся в возможности ее изменения любым субъектом;
2) свойство информации, заключающееся в возможности изменения только единственным пользователем;
3) свойство информации, заключающееся в ее существовании в виде единого набора файлов;
4) свойство информации, заключающееся в ее существовании в неискаженном виде(неизменном по отношению к некоторому фиксированному ее состоянию).
6.Утечкаинформации - это:
1) несанкционированное изменение информации, корректное по форме,
содержанию, но отличное по смыслу;
2) ознакомление постороннего лица с содержанием секретной информации;
3) потеря, хищение, разрушение или неполучение переданных данных;

Тестовые задания (ОПК-7 Владение навыками):
1. Уровень секретности–это:
1) ответственность за модификацию и НСД информации;
2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов;
2. Угроза–это:
1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов;
2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов.
3. Универсальная компьютерная система состоит из:
1) операционной системы, сетевого программного обеспечения;
2) операционной системы, сетевого программного обеспечения и системы управления базами данных;
3) операционной системы, системы управления базами данных;
4) сетевого программного обеспечения и системы управления базами данных.
4. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение или к ликвидацию различных видов угроз безопасности объектам защиты–это называется:
1) системой угроз;
2) системой защиты;

3) системой безопасности;
4) системой уничтожения.
5. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется:
1) политикой информации
2) защитой информации
3) политикой безопасности
4) организацией безопасности
6. Группы, на которые делятся средства защиты информации- это:
1) физические, аппаратные, программные, криптографические, комбинированные;
2) химические, аппаратные, программные, криптографические, комбинированные;
3) физические, аппаратные, программные, этнографические, комбинированные;

Тестовые задания (ПК-5 Владение навыками):
1. Компьютерный вирус –это:
1) разновидность программ, которые способны к размножению;
2) разновидность программ, которые самоуничтожаются;
3) разновидность программ, которые не работают;
4) разновидность программ, которые плохо работают.
2. В зависимости от деструктивных возможностей, вирусы подразделяются на:
1) сетевые, файловые, загрузочные, комбинированные;
2) безвредные, неопасные, опасные, очень опасные;
3) резидентные, нерезидентные;
4) полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы.
3. ЭЦП предназначено для:
1) обеспечение целостности;
2) обеспечение доступности;
3) обеспечение авторства;
4) обеспечение конфиденциальности;
5) обеспечение неотказуемости
4. Размер ключа шифрования определяется:
1) используемым криптографическим алгоритмом;
2) методом шифрования;
3) стойкостью алгоритма шифрования.
5. Стойкость шифра определяется:
1) вычислительной сложностью задачи криптоанализа;
2) максимально достижимым уровнем секретности;
3) алгоритмом шифрования.
6. Криптоалгоритм RSA применяется:
1) в симметричных криптосистемах;
2) в асимметричных криптосистемах;
3)при хэшировании.
7. Криптоалгоритм DES применяется:
1) в симметричных криптосистемах;
2) в асимметричных криптосистемах;
3)при хэшировании

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг-план

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Раздел 1.				
Текущий контроль				**25**
1. Устный опрос	2	5	0	10
2. Решение задач у доски	3	3	0	15
Рубежный контроль				**25**
1. Тестирование	5	5	0	25
Раздел 2.				
Текущий контроль				**25**
1. Устный опрос	2	5	0	10
2. Решение задач у доски	3	3	0	15
Рубежный контроль				**25**
1. Тестирование	5	5	0	25
Поощрительные баллы				**10**
1. Студенческая олимпиада				**2**
2. Публикация статей				**3**
3. Участие в конференции				**3**
4. Активная работа на аудиторных занятиях				**2**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			**0**	**–6**

2. Посещение практических занятий			**0**	**–10**
Итоговый контроль				
Зачет				
Итого			**0**	**110**

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 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.